Computers and Electrical Engineering 81 (2020) 106504

Contents lists available at ScienceDirect

Computers and Electrical Engineering

journal homepage: www.elsevier.com/locate/compeleceng

An Edge Computing-enhanced Internet of Things Framework for Privacy-preserving in Smart City☆

Mehdi Gheisari[a], Guojun Wang[a,*], Shuhong Chen[a,b]

[a] School of Computer Science, Guangzhou University, Guangzhou 510006, China
[b] Department of Electrical and Computer Engineering, University of Florida, Gainesville, FL 32611, USA

ARTICLE INFO

Article history:
Received 13 November 2018
Revised 17 September 2019
Accepted 30 October 2019
Available online 21 November 2019

Keywords:
Privacy-preserving
Smart city
Ontology
Edge computing
Internet of things
Owner
Privacy
IoT
Cloud computing

ABSTRACT

To supervise massive generated data by the Internet of Things (IoT) efficiently, we face two issues that should be addressed which are: (1) heterogeneity or satisfying diversity among IoT devices, and (2) privacy-preserving or preventing unintentional disclosure of sensitive data. Through observation, we found that existing solutions apply one common privacy-preserving rule for all devices while they address the heterogeneity issue separately that lead to unappealing performance. In this paper, we propose a framework for addressing the heterogeneity issue and privacy-preserving of IoT devices at the network edge using a novel proposed ontology data model. Besides, it leverages the proposed ontology to obtain a privacy-preserving method by frequently changing the privacy-preserving behaviors of IoT devices. Through simulation, we show that our solution overhead is less than 9 percent in the worst situation so that it is affordable to most IoT devices in one of its applications that is smart city.

1. Introduction

One of the two-sword technologies on our daily life is Internet of Things(IoT) that has positive and negative affects [1,2]: positively, it can provide a lot of high-level services to the end-users depending upon its spanning area. Negatively, due to rural population chooses towns because of the concentration of resources and the world population is growing at an exponential rate (based on the predictions, cities will inhabit half of the world population by 2050 [3]), it comes up with immense pressure on managing the massive amount of generated data efficiently.

Facilitating IoT with typical cities make a crucial point of interest for the local government and politicians even now, let alone the population of cities will increase much soon [4,5]. Hence, a variety of governing bodies invest massively for disposing related problems of effective management of cities called “Smart City” [6]. In short and straightforward, a smart city leverages IoT with the aim of:

1. Enhancing different aspects of services for citizens.
2. Satisfying the city community’s changing needs.
3. Collaboration with other communities.

☆ This paper is for regular issues of CAEE. Reviews processed and approved for publication by the Editor-in-Chief.

* Corresponding author: Guojun Wang (csgjwang@gzhu.edu.cn).
E-mail address: csgjwang@gzhu.edu.cn (G. Wang).

https://doi.org/10.1016/j.compeleceng.2019.106504
0045-7906/

In the smart city environment, billions of various IoT devices made by different vendors share their sensed data intending to provide quality services. Due to which, two main issues come up: (1) Heterogeneity: stems from the diversity of IoT devices, each device has its own characteristic and (2) Privacy-preserving: refers to unintentional disclosure of data [7].

One paradigm that helps us to address IoT devices shortcomings such as being energy-constraint is Cloud Computing (CC) that refers to on-demand delivery of analysis power, database storage, applications, and other Information Technology (IT) resources [8]. It leverages various services like software development platforms, and servers over the Internet. It brings some significant capabilities like unlimited scaling, elasticity by using shared services. It is an infrastructure that can provide the IoT infrastructure to obtain better performance such as it supports the IoT environment to overcome its limited computing and storage characteristics [9]. It is worth to mention that leveraging Cloud Computing with IoT is in its infancy stage, particularly in the smart city domain; most of the proposed solutions have not entirely used the advantage of the combination of these technologies.

Recently, a new paradigm has emerged that is an extension of Cloud Computing called “Edge-Computing”. It is known for performing applications in an approximately real-time manner by taking some part of an application such as its data, or services away from one or more central nodes to the other logical parts, the “edge” of the network [1].

From knowledge representation prospect, we can leverage a data model called “Ontology” for an explicit expression of a conceptualization. Using the ontology, we can represent environmental domain information. Moreover, we can use it for automatic machine processing for those machines that do not have any perception [10,11]. It depicts a set of representational primitives to scheme a knowledge/discourse domain. These representational primitives are commonly classes or sets, relationships or relations among class members, and attributes or properties [12]. So, since it brings a unified abstract of the whole system, it can address the diversity various IoT devices. Even IoT devices from same vendor can provide heterogeneity like they can provide data by different formats.

In order to address the privacy-preserving efficiently while addressing the heterogeneity issue, we propose a novel ontology to keep privacy information of devices. Then, based on the proposed ontology, we propose a privacy-preserving method on top of it that changes the applying privacy-preserving rules of devices frequently.

The major contributions of this paper are mainly four-fold:

1. We propose an architecture for privacy-preserving while addressing the heterogeneity issue at the network edge in order to achieve an efficient IoT-based smart city. To obtain the said objective and depict its efficiency:
2. Firstly, we have proposed an ontology for the IoT-based smart city environment in order to develop a united view among IoT devices that includes not only their properties but also their privacy rules’ characteristics, addressing the heterogeneity problem.
3. Secondly, we have proposed a method based on the created ontology to preserve the privacy of IoT devices in the smart city that produce sensitive data at the edge of the network. This is obtained by changing the privacy behavior of each device dynamically.
4. Finally, we have validated our solution to show that most IoT devices in our scenario can afford the amount of overload imposed on the system. So, it can widely be used in highly dynamic environments such as the smart city.

This paper is organized as follows: Section 2 describes related work. Section 3 depicts an overview of the ecology. Section 4 focuses on our proposed solution in detail, its ontology and privacy preserving algorithm and evaluation of them. Finally, Section 5, end of this paper, concludes the paper and also presents possible future work to have a more efficient smart city.

2. Related work

Vendors of IoT devices desire to develop smart IoT devices based on their benefits that will lead to heterogeneity of producing devices and possible conflicts between diverse generated platforms. Meanwhile, the generated data from IoT devices should remain safe so that sensitive data will not be misused by any adversaries. These two issues create significant challenges in providing a trustable environment. Here, in the related work, we focus on the literature that considers the privacy-preserving of IoT devices that produce sensitive data while trying to address the heterogeneity issue.

In [13], authors projected a novel cloud architectural model that is developed to enhance the interoperability of various devices or services provided by several different vendors for smart homes that is based on the IoT. Their model is multi-layer. Furthermore, they used the ontology data model for knowledge representation of the smart homes domain to address the heterogeneity among them. They also not only propose a security framework through their proposed ontology but also leveraging the Semantic Web Rule Language (SWRL) to describe the reasoning rules to provide quality services through more efficient interoperations of the various devices. Despite their system advantages, it has several disadvantages such as authors have not evaluated their solution based on the amount of the overload. So, it is not clear that their solution is affordable to IoT devices that are resource constraint or not. Moreover, their answer is slow so that it cannot be applied in real-time demanded environments such as the smart city. And, they did not evaluate how much their model can resist against unintentional disclosure of data or privacy-preserving level.

Authors in [14] proposed a solution for doing data aggregation while preserving the privacy of fog computing-enhanced IoT devices. They employed several techniques in order to enhance data aggregation process while preserving the privacy. They employed (1) one-way hash chain for authenticating IoT devices efficiently and filtering false data in the early stage

which is injected by external attackers, (2) Chinese Remainder Theorem for aggregating generated data by various IoT devices. They also leveraged the Homomorphic Paillier Encryption method for providing security of data as well. Moreover, in order to provide enhanced privacy, they leveraged differential privacy techniques. Some of the advantages of their proposed solution include: (1) it is fault-tolerant, (2) it solves the heterogeneity issue in partial mode. On the other hand, their solution does not provide standardized understanding among IoT devices so that it cannot address the heterogeneity issue effectively. Moreover, their solution applies one common privacy-rule, differential privacy, for all IoT devices that causes an unacceptable amount of unintentional disclosure of sensitive data.

Authors in [15] proposed an ontology for privacy-preserving of IoT devices in the smart city. Then, on top of that we propose a privacy-preserving method based on the stored information in ontology. We calculated only the amount of computational cost overhead for evaluation. On major drawback is that the privacy-preserving method can be recognized by adversaries even simple one. In other words, a portion of private information may still be unintentionally disclosed by untrusted entities.

In [16], authors proposed the idea of anonymous authentication protocol for preserving the privacy of IoT devices in target-driven applications. With the usage of an anonymous authentication method, we can authorize only those IoT devices to have access to the system if they deserve without their disclosure of their identities. So, only the anonymous approved IoT devices can leverage the network. Thus, it can bring an efficient IoT-based smart city environment while anonymous IoT devices are authenticated. Based on the evaluation results, their system can be applied to the IoT applications. Their anonymous credential system is implemented. Advantages of their system can be described as follows:

- Their solution can control the group of users from which collect data through leveraging access control policies based on the attribute of users.
- Their solution can interact with the users in a completely anonymous manner, no disclosure of private data and attributes.
- Their method is decentralized and does not rely on a central center, so it is robust against single point failure.

Their system has several disadvantages such as it causes unacceptable privacy-preserving level stems from the fact adversaries can penetrate the system due to it is static. Another one is that they did not pay attention to the lifetime of the system and calculate the amount of overload imposed on it.

To address the proposed methods' drawbacks of the related work and to provide a safer smart city, we offer a solution for privacy-preserving, changing privacy rules of devices time by time in the smart city environment, while addressing heterogeneity issue. Moreover, our solution performs at the network edge in order to address the on-demand services.

3. System overview

In order to describe the ecology of our solution, at first, we explain the IoT-based smart city, and then, its integration with the Edge-Computing.

3.1. IoT-based Smart City

IoT refers to connecting objects with each other through the Internet to provide high-level services. Objects can be a human, a non-human creature or any handicraft that is equipped with a unique identifier such as IP [17]. It aims to provide quality services by collaborating of IoT devices, the produced data must be shared with other devices, that lead to several challenges such as privacy and heterogeneity [18]. If we can address its challenges, we will have more motivation in utilizing its provided services. In our scenario, we discuss the issues at the edge of the network, such as Fire stations, Base Transceiver Stations (BTSs), hospitals, schools, and so on.

On the other hand, according to World Health Organization statistics, the population of cities will be twice by 2050 [19]. Metropolitan Cities are currently dealing with increasing pressing challenges such as transportation and citizen mobility, city economic growth, environmental sustainability and management let alone the population increases [20,21]. To deal with the said problems, a new paradigm appeared called "Smart City" that leverages ICT as the basis of the whole town, its property, its channels of communication and other equipment.

3.2. Edge-Computing

In order to have a more efficient smart city while we are able to respond to on-demand queries, we equip the smart city with the Edge-Computing paradigm. That is, servers are taking off their pressure on centralized data centers by moving data centers nearer from the Cloud space to the network edge or close to the clients [22]. It speeds up the storage processing, approximately in a real-time manner. We can perform data analysis more efficiently without sending them to centralized data centers in the cloud space. Processing at the edge of the network causes better performance and faster average response time. Thus, this paradigm provisions more excellent quality of services for IoT applications [23]. Fig. 1 shows the info-graphic of IoT, Cloud Computing space, and Edge-Computing.

As far as Fig. 1 depicts, Edge-computing is located between Cloud Computing and IoT paradigms. Thus, it can serve on-demand services at the edge of the network. We can enhance one crucial application of IoT, smart city, with the Edge-computing that is described as follows:

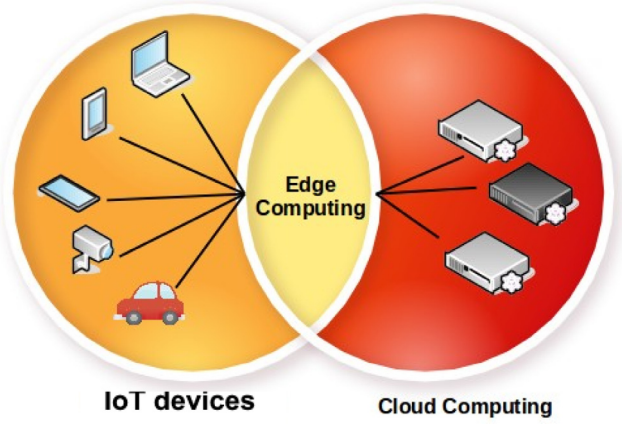

Fig. 1. IoT, Cloud Computing space, and Edge-Computing ecology.

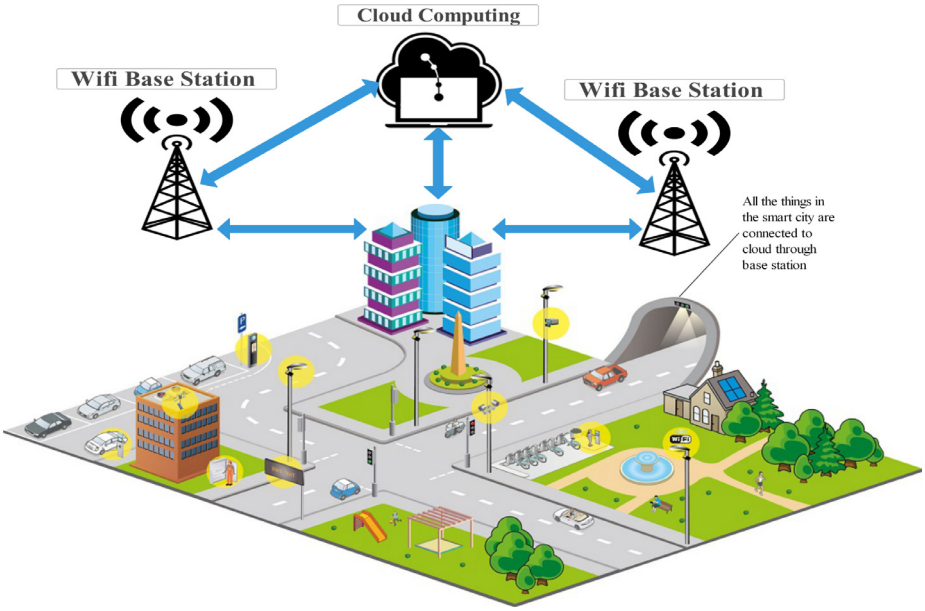

Fig. 2. Facilitated city with IoT.

3.3. Edge-computing enhanced IoT-based smart city

Fig. 2 shows Edge-computing enhanced IoT-based smart city concept in a schematic form. In the environment, each device sends its data to an edge node such as BTSs. Next, this edge node processes the collected data in real-time mode. Then, it will send the processed data to the Cloud Computing environment for further analysis [24].

As Fig. 2 shows, IoT devices of the smart city such as smart skyscrapers, smart shops, and smart homes collaborate with edge nodes to provide high-level services. In other words, each structure shares its data like its current status with the edge node that can be a BTS with the aim of providing high-level joint data decisions [25,26]. Our solution, ontology server located at the edge node, is described as follows:

4. Ontology server

This section discusses our proposed ontology server that is based on a proposed ontology to preserve the privacy of IoT devices' data in a smart city environment. In detail, the ontology server includes two parts: (1) ontology, and (2) a privacy-preserving procedure. The ontology- a data storage model- is designed by shaping the correlative perceptions of the smart city devices' information and their privacy properties to address the heterogeneity issue and paves the way for the introduction of the privacy-preserving procedure. For the privacy-preserving procedure part- based on the created ontology information- we frequently change the applying privacy behaviors of the IoT devices.

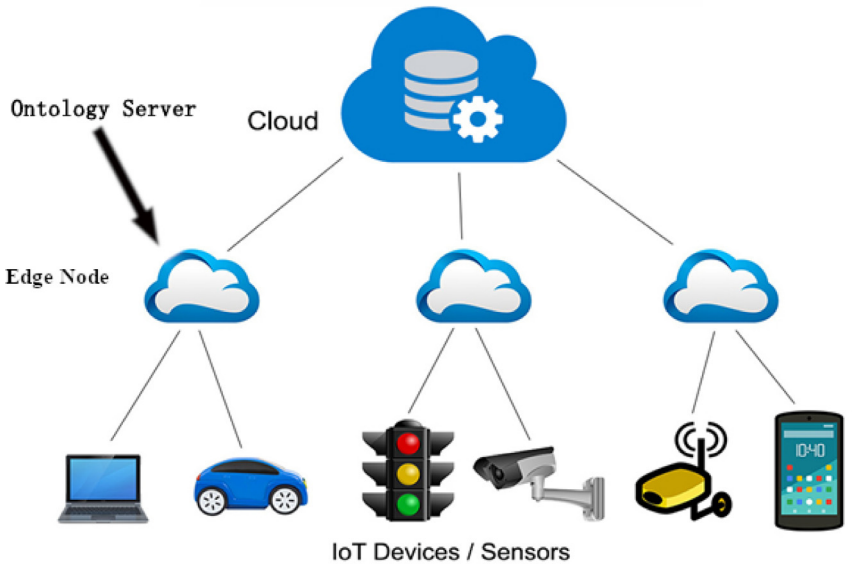

Fig. 3. Ontology server located at the edge node.

Fig. 3 depicts the ontology server ecology.

As Fig. 3 shows, after sensing their sensitive data and perturbing their data, IoT devices send their data to the edge of the network for real-time analysis. Then, they send them to the Cloud Computing space for further analysis such as data mining.

4.1. Ontology

In the IoT domain, we are facing several challenges in providing efficient IT-supported services such as (1) heterogeneity of devices, services, data formats, developed by solutions from different vendors, (2) privacy-preserving that refers to the unintentional disclosure of sensitive data; it is likely that these IoT devices generate sensitive data while leading to information leakage. These challenges make a barrier to the widespread application of IoT. Thus, we should propose solutions in order to address IoT challenges. One solution that offers a prominent knowledge base while it is united with the raw sensor data called "ontology" [27,28]. Moreover, it can be used for privacy rules demonstration while solving the heterogeneity issue of various devices as well. It supports a high-level abstraction for addressing privacy objectives. Thus, in the proposed ontology, we depict IoT devices' information along with their possible applying privacy information. In detail, we store four information in the ontology: (1) the applying privacy rule of each device, (2) its privacy rule lifetime, how long the privacy rule is valid, (3) its owner, who owns the device, and (4) its value. We store the owner of devices with the aim of misguiding adversaries in order to make confusion in which data is the sensitive one. It is evident that the proposed ontology can be enriched by introducing new classes, associations, and properties so that we are able to recommend more efficient privacy-preserving solutions.

Fig. 4 shows the proposed ontology, a module of the ontology server, to satisfy real-time demands in the IoT-based smart city domain. It is created by Protege software version 5.2.0.

Smart city class covers smart city devices, smart city alarm devices, and applicable privacy-preserving information of them in the smart city. The privacy class represents the content privacy that covers the privacy information of sensed data produced by IoT devices. Moreover, the context privacy class depicts information about privacy of non-sensed data from IoT devices. The Privacy Rules class covers possible applying privacy-preserving rules by IoT devices that in our scenario are Data Swapping, Random Noise, and Data Micro Aggregation. In other words, there are three possible privacy-preserving rules that each device can apply, fulfilled when the system starts.

The second layer class of the proposed projected ontology covers smart city devices information that is divided into five sub-classes: (1) camera devices, (2) tilt devices, (3) speed devices, (4) temperature devices, and (5) color devices. "Camera" class contains 5 camera instances, numbered from one to five. They visually monitor the environment. Moreover, the speed class individuals sense the speed of the target objects and record them if any unusual situation occurs. It consists of two speed measurement devices called "Speed sensor" and "Speedsensor2". Besides, tilt sensor class individuals are in charge of measuring the steep of targets. They report unusual steep conditions. The next class is the Temperature one that includes

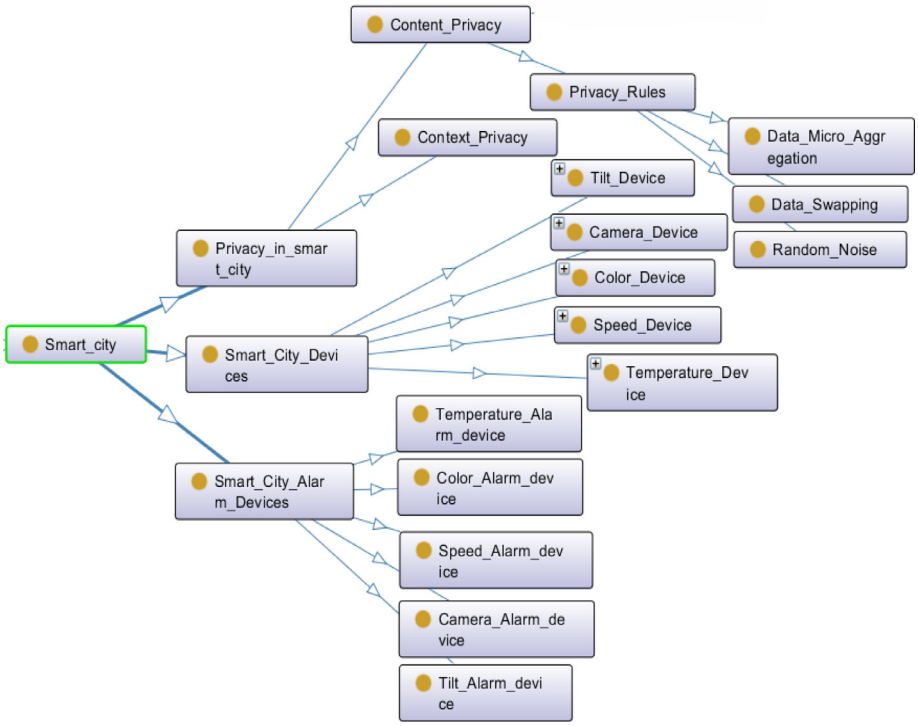

Fig. 4. Abstract point of privacy rule ontology.

temperature IoT devices while they have the duty of sensing and reporting the irregular sensed temperature conditions like possible fire in open areas. And, the last class in our proposed ontology is the color class that includes two individuals: “Color sensor” and “Color sensor2”.

In the defined ontology, we store another class that is associated with the smart city alarm devices. Individuals aim to be triggered when they detect abnormal conditions. Due to we assumed that five types of IoT devices exist, we have five alarm classes that have mutual relations with their corresponding smart city device classes.

In brief, we have twelve IoT devices in our scenario from 5 different categories that are cameras, speed sensors, temperature sensors, color sensors, and tilt ones [29]. Each one has four properties, its privacy rule method, its privacy rule lifetime, its data type, and its owner. For instance, the “camera1” has the data type of string with the value of Super-Zoom; its privacy method is one that refers “Micro Aggregation” method as shown in Table 2; its privacy rule lifetime is 5 that displays after five times slices, the privacy rule of the IoT device should be changed to another selected privacy rule. Moreover, the owner of this camera is Traffic Manager (TM) of the city. In our scenario, two types of data are flowing: (1) the owner information, and (2) the original data. The owner information is used only because of misguiding adversaries, malicious attempts that are trying to find the generated sensitive data. In other words, the adversaries should differentiate which data is the real sensitive data and which one is non-useful data, ownership information. Thus, with the usage of the owner information, the adversaries get confused which data is useful data and which one not, owner information.

In our scenario, the second device is camera number two that its privacy method number is three, an assumption, denotes Random Noise based on the Table 2. Its privacy lifetime is four that it shows after four time slices, the applying privacy-preserving rule should be changed. Its type is a string with the data value of Compact, and its owner is the TM of the city. This process is valid for all of the smart city devices accordingly.

Table 1 shows all of the instances in schematic form; TM refers to the Traffic Manager, CM refers to the City Manager, F to the Forecaster, PL denotes Privacy rule Lifetime, and PM relates to its current Privacy Method of the IoT device.

The privacy policy approaches and their equivalent numbers are shown in Table 2.

As Table 2 depicts, we have three numbers that show privacy methods. Number one specifies that the device is using the Data Micro Aggregation privacy technique. Number two indicates the Swapping, and the last one, number 3, shows the IoT device is using the Random Noise method as its privacy-preserving method. For example, If the applying privacy-preserving method of an IoT device is Data Micro Aggregation, ontology server instead of sending “Micro Aggregation” text to the IoT device, it will send its equivalent number, number 1 based on the Table 2, and vice versa. We assume that each IoT device has built-in Table 2 information. This assumption can be removed so that the devices do not need to have built-in Table 2 information. And, this can be achieved if the ontology server notifies them when the system starts.

Table 1
IoT devices in the smart city and their property values.

Device ID	Device type	PM	PL	Owner
Camera 1	Super-Zoom	1	5	TM
Camera 2	Compact	3	4	TM
Camera 3	Multiplane camera	2	4	TM
Camera 4	Pin speck camera	3	2	TM
Camera 5	Pool safety camera	1	3	TM
Color Sensor	TCS34725	2	4	CM
Color Sensor 2	TCS34725	3	4	CM
Tilt Sensor	AT407	2	2	TM
Speed Sensor	Variable Reluctance	3	1	TM
Speed Sensor 2	Intrinsically Safe Speed Sensors ATEX, IECEx, and CSA Certified	2	2	TM
Temperature Sensor	Celsius Scale Temperature Sensor	3	2	F
Temperature Sensor 2	NTC thermistor	2	3	F

Table 2
Privacy numbers and their equivalents.

Privacy numbers	Privacy methods
1	Micro Aggregation
2	Swapping
3	Random Noise

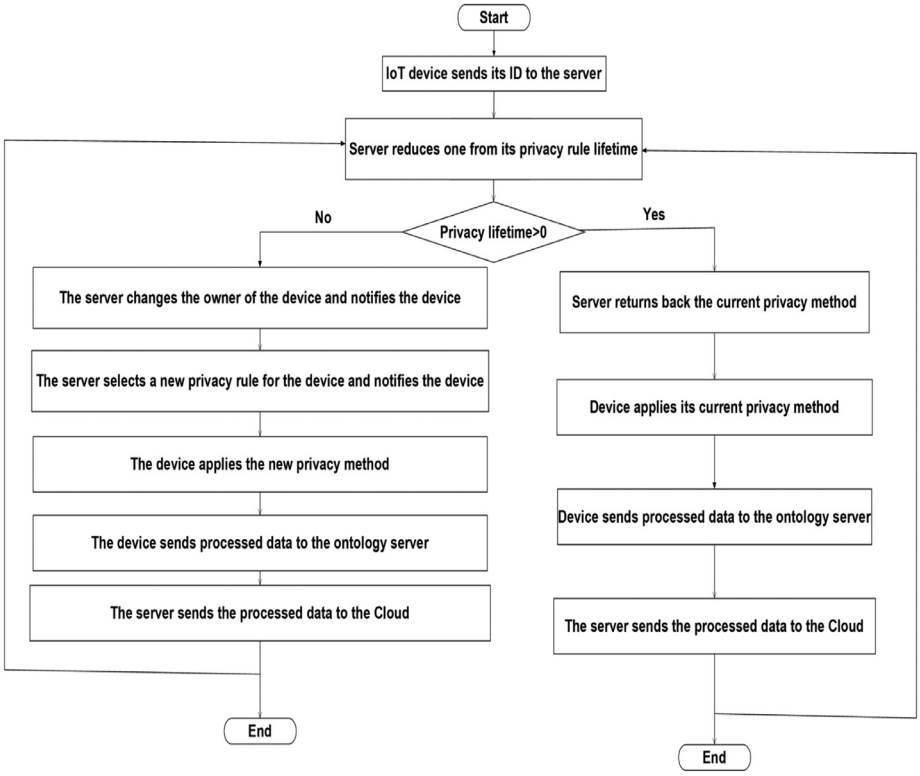

Fig. 5. Flow chart of the privacy-preserving procedure.

4.2. Privacy-preserving procedure

After creating the ontology that includes IoT devices' knowledge, in this section, we mount our privacy-preserving method on top of it. The flowchart of the mounting proposed privacy-preserving rule is shown in the Fig. 5.

At first, each IoT device sends its ID to the server includes ontology. Server deducts one from its privacy rule lifetime. After decreasing, if the lifetime is positive, the server returns the current privacy method in order to the device applies it. But, if the privacy rule lifetime becomes zero, it will change the owner of the device, randomly, in order to misguide

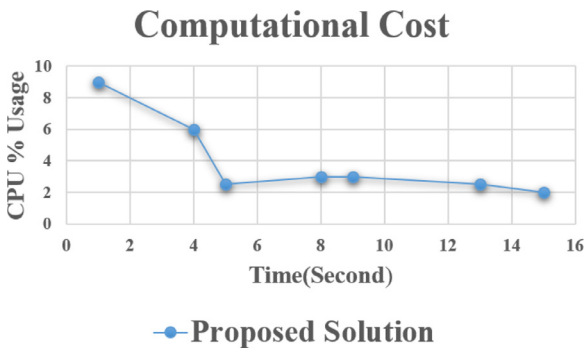

Fig. 6. Computational cost.

adversaries and notifies the device about this change. Then, the server will choose another proper privacy rule to be applied by the device and sends back its equivalent number that is selected randomly in our scenario. More investigation is needed to find the best next privacy-preserving rule for each type of device, future work. Then, the IoT device sends its processed data after applying the selected new privacy technique to the ontology server that is located at the edge of the network. From there, the data will be sent to the Cloud Computing environment for further analysis.

5. Performance evaluation

In this section, we focus on evaluating our ontology server solution, its performance, and the amount of effectiveness.

For simplicity of simulation, we show each IoT device as a bulb. We depicted each privacy rule as the color of it. The applying privacy rule of an IoT device has three choices: green, blue, yellow. Every device has its privacy-preserving rule lifetime that shows how long the applying privacy rule or color is valid. Every time slice, the lifetime is subtracted. If the ontology server, located at the edge of the network, finds the lifetime equals to zero, the server changes the applying privacy rule of the device and its owner randomly to prevent adversaries from misusing the produced information of the IoT devices in the smart city.

However, from the coding point of view, each device has a cycle that shows its privacy method past time. In the beginning, all bulbs are off when all devices start. Next, the server allocates each device a privacy method and a privacy rule lifetime. The server which is located at the edge of the network periodically checks the devices' privacy rule lifetime. If any privacy rule lifetime of the devices becomes zero, then the ontology server changes the owner of the device and, next, it selects another privacy rule, color, arbitrarily, and will appoint to the device. The device will apply the new privacy method and sends it to the ontology server. In turn, it will send to the Cloud Computing environment.

For evaluation, as the first step, we only calculated the amount of CPU overload on the system that can be extended to more evaluation metrics, as future work due to the fact if the proposed solution is very costly, it may not be affordable to IoT devices that are resource-constraint. Fig. 6 shows the CPU usage of all devices during the time.

As it is understandable, the amount of the computational cost is less than 9.0 percent. Nine percent overload is suitable for huge, highly-dynamic projects such as smart cities. If the overload is tolerable, it means that we can apply it quickly to the dynamic environments that sensitive data is produced in high volumes, so that many users can use it. But, one drawback of our solution is that if the number of devices increases, the performance may reduce significantly since in our solution, we did not pay attention to the number of devices.

Our solution can be defined as complementary to traditional privacy-preserving methods. In typical systems, usually, we have one static privacy rule for the entire system. In general, the system is static from the privacy rule prospect. On the contrary, the ontology server brings dynamism to each IoT device that has a data type, a privacy rule, the owner, and a privacy lifetime; it shows how long the privacy method is valid. From the abstract point of view, ontology server provisions dynamism from the privacy rule aspect while it solves the heterogeneity issue at the edge of the network. Thus, if the security mechanism cannot hinder the unwanted parties, our solution can support the security mechanism and pushes the adversaries back.

6. Conclusion and future works

In this paper, we addressed two significant challenges in the IoT-based smart city environment that are heterogeneity and privacy-preserving. For addressing the heterogeneity issue, we proposed an ontology that not only includes IoT devices and alarm devices information but also the privacy information of them. Moreover, for the privacy-preserving issue, based on the ontology information, we frequently changed the privacy behaviors of IoT-based smart city devices. All these processes are performed at the edge of the network that provides services in an approximately real-time manner. We evaluated the efficiency of our solution based on the amount of imposing overload, which is one of the most essential evaluation metrics

that should be calculated. We showed that our solution is affordable to many IoT devices that are not severe resource-constraint; it imposes utmost 9.0 percent overload. We also showed that our solution might not address the scalability issue. Some of future works that can be done are: (1)finding the best possible privacy rules for each IoT device based on the machine learning approaches, (2) taking heed on the other evaluation metrics such as the amount of the penetration rate of the system, (3) how much the system is robust against unintentional sensitive data disclosure. Additionally, another future work is proposing a solution that is scalable. Moreover, we have a plan to evaluate our proposed method when the devices are moveable.

Declaration of Competing Interest

There is not any conflict of interest between authors.

Acknowledgment

National Natural Science Foundation of Chinaunder Grants 61632009 and 61472451, Guangdong Provincial Natural Science Foundation under Grant 2017A030308006 High-Level Talents Program of Higher Education of Guangdong Province under Grant 2016ZJ01. Moreover, this research is supported by China Scholarship Council (CSC) Visiting Scholar Foundation,Grant Number: 201808440071.

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.compeleceng.2019.106504.

References

[1] Liu Q, Wang G, Liu X, Peng T, Wu J. Achieving reliable and secure services in cloud computing environments. Comput Electr Eng 2017;59:153–64.
[2] Liu Q. Enabling cooperative privacy-preserving personalized search in cloud environments. Inf Sci 2019;480:1–13.
[3] Gheisari M, Wang G, Khan WZ, Fernndez-Campusano C. A context-aware privacy-preserving method for iot-based smart city using software defined networking. Comput Secur 2019:101470. doi:10.1016/j.cose.2019.02.006. http://www.sciencedirect.com/science/article/pii/S0167404818313336.
[4] M G, G W, S C. Iot-SDNPP: a method for privacy-preserving in iot-based smart city with software defined networking. In: 18th international conference on algorithms and architectures for parallel processing. Springer; 2018.
[5] Hendalianpour A, Fakhrabadi M, Zhang X, Feylizadeh MR, Gheisari M, Liu P, Ashktorab N. Hybrid model of IVFRN-BWM and robust goal programming in agile and flexible supply chain, a case study: Automobile industry. IEEE Access 2019;7:71481–92.
[6] Mollah MB, Azad MAK, Vasilakos A. Security and privacy challenges in mobile cloud computing: survey and way ahead. J Netw Comput Appl 2017;84:38–54.
[7] Gheisari M, Wang G, Bhuiyan MZA. A survey on deep learning in big data. In: 2017 IEEE international conference on computational science and engineering (CSE) and IEEE international conference on embedded and ubiquitous computing (EUC), vol. 2; 2017. p. 173–80.
[8] Gheisari M, Alzubi J, Zhang X, Kose U, Saucedo JAM. A new algorithm for optimization of quality of service in peer to peer wireless mesh networks. Wireless Netw 2019:1–9.
[9] Wang F, Jiang W, Li X, Wang G. Maximizing positive influence spread in online social networks via fluid dynamics. Future Gener Comput Syst 2018;86:1491–502.
[10] Wang F, Li J, Jiang W, Wang G. Temporal topic-based multi-dimensional social influence evaluation in online social networks. Wireless Pers Commun 2017;95(3):2143–71.
[11] Arif M, Wang G, Bhuiyan MZA, Wang T, Chen J. A survey on security attacks in VANETs: communication, applications and challenges. Veh Commun 2019:100179.
[12] Mollah MB, Zeadally S, Azad MAK. Emerging wireless technologies for Internet of Things applications: opportunities and challenges. Cham: Springer International Publishing; 2019. p. 1–11. doi: 10.0007/978-3-319-32903-1.
[13] Tao M, Zuo J, Liu Z, Castiglione A, Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for iot-based smart homes. Future Gener Comput Syst 2018;78(Part 3):1040–51.
[14] Lu R, Heung K, Lashkari AH, Ghorbani AA. A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced iot. IEEE Access 2017;5:3302–12.
[15] Gheisari M, Pham Q, Alazab M, Zhang X, Fernández-Campusano C, Srivastava G. Eca: an edge computing architecture for privacy-preserving in iot-based smart city. in IEEE Access 2019;7:155779–86.
[16] Alcaide A, Palomar E, Montero-Castillo J, Ribagorda A. Anonymous authentication for privacy-preserving iot target-driven applications. Comput Secur 2013;37:111–23.
[17] Rezaeiye P, Rezaeiye pp, Beig EFGM, Mohseni H, Kaviani R, Gheisari M, Golzar M. Agent programming with object oriented (c++). In: Electrical, computer and communication technologies (ICECCT), 2017 second international conference on. IEEE; 2017. p. 1–10.
[18] Kia MMM, Alzubi JA, Gheisari M, Zhang X, Rahimi M, Qin Y. A novel method for recognition of persian alphabet by using fuzzy neural network. IEEE Access 2018;6:77265–71.
[19] Peng S, Wang G, Zhou Y, Wan C, Wang C, Yu S. An immunization framework for social networks through big data based influence modeling. IEEE Trans Dependable Secure Comput 2018. 1–1
[20] Alzubi A, Yaghoubi JA, Gheisari M, Qin Y. Improve heteroscedastic discriminant analysis by using CBP algorithm. In: Algorithms and architectures for parallel processing. Cham: Springer International Publishing; 2018. p. 130–44.
[21] Alzubi JA, Shahabi AS, Fernndez-Campusano C, Gheisari M, Qin Y. A solution for cluster leader selection in wireless sensor networks. In: 2018 24th international conference on automation and computing (ICAC); 2018. p. 1–6.
[22] Sethuraman RMMJ, Alzubi J, Manikandan R, Gheisari M. Eccentric methodology with optimization to unearth hidden facts of search engine result pages. Recent Patents Comput Sci 2018:11:1.
[23] Gheisari M, Esnaashari M. Data storages in wireless sensor networks to deal with disaster management. In: Emergency and disaster management: concepts, methodologies, tools, and applications. IGI Global; 2019. p. 655–82.
[24] Jafari M, Wang J, Qin Y, Gheisari M, Shahabi AS, Tao X. Automatic text summarization using fuzzy inference. In: 2016 22nd international conference on automation and computing (ICAC); 2016. p. 256–60.

[25] Zhang S, Wang G, Liu Q. A dual privacy preserving scheme in continuous location-based services. In: 2017 IEEE Trustcom/BigDataSE/ICESS; 2017. p. 402–8.
[26] Ashourian M, Mehdi G, Ali H. An improved node scheduling scheme for resilient packet ring network. Majlesi Journal of Electrical Engineering 2015;9.2:43.
[27] ARIF M, WANG G, BALAS VE. Secure VANETs: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud Inf Control 2018;27(2):235–46.
[28] Noor F, Sajid A, Shah SBH, Zaman M, Gheisari M, Mariappan V. Bayesian estimation and prediction for burr-rayleigh mixture model using censored data. Int J Commun Syst 2019;0(0):e4094.
[29] Gheisari M, Bahekmat M, Setoodeh HR, Khajehyousefi M. A comparison with some sensor network storages. In: International conference on computer and computer intelligence (ICCCI 2011). ASME Press; 2011.

Mehdi Gheisari is a Ph.D. candidate, in defence procedure, in computer science at Guangzhou University since September 2016. He is currently doing research on Privacy-preserving in IoT. Prior to that he was with the Islamic Azad University where he was serving in the capacity of lecturer in the department of computer science. There, he worked on Wireless Sensor Networks. Furthermore, he has published several papers in several domains with his colleagues in highly ranked journals and several ranked conferences. He also served in academic works such as reviewing papers from several well-known venues such as IEEE communication magazine, TPC of several conferences and so on. His profile can be accessed via: https://scholar.google.com.sg/citations?user=tmWQt9UAAAAJ&hl=en.

Guojun Wang received BSc in Geophysics, MSc in Computer Science, and PhD in Computer Science from Central South University, China. He is currently a Professor at Guangzhou University, China. He was Professor at Central South University, China; Visiting Scholar at Temple University and Florida Atlantic University, USA; Visiting Researcher at The University of Aizu, Japan; and Research Fellow at The Hong Kong Polytechnic University.

Shuhong Chen is an Associate Professor of Computer Science at Guangzhou University, China. She is also a visiting scholar at University of Florida, USA. Her major research interests include trust evaluation, mobile social networks, and performance analysis. She has served as General Chair for UbiSafe from 2017 through 2019, Organizing Chair for IEEE ISPA 2017, Workshop Chair for UIC 2019.