IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 26, 2019, accepted August 2, 2019, date of publication August 23, 2019, date of current version November 6, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2937177

ECA: An Edge Computing Architecture for Privacy-Preserving in IoT-Based Smart City

MEHDI GHEISARI[1,2,3], QUOC-VIET PHAM[4], MAMOUN ALAZAB[5], XIAOBO ZHANG[1], CHRISTIANFERNÁNDEZ-CAMPUSANO[6], AND GAUTAM SRIVASTAVA[7,8]

[1]Faculty of Automation, Guangdong University of Technology, Guangzhou 510006, China
[2]School of Computer Science, Guangzhou University, Guangzhou 510006, China
[3]Young Researchers and Elite Club of Parand Branch, Islamic Azad University, Parand 3761396361, Iran
[4]High Safety Core Technology Research Center, Inje University at Gimhae-si Campus, Gimhae 50834, South Korea
[5]College of Engineering, IT, and Environment, Charles Darwin University, Casuarina, NT 0810, Australia
[6]Department of Computer Architecture and Technology, University of the Basque Country UPV/EHU, 20018 Donostia-San Sebastin, Spain
[7]Department of Mathematics and Computer Science, Brandon University, Brandon, MB R7A 6A9, Canada
[8]Research Center for Interneural Computing, China Medical University, Taichung 40402, Taiwan

Corresponding author: Xiaobo Zhang (zxb_leng@gdut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61632009 and Grant 61472451, in part by the Guangdong Provincial Natural Science Foundation under Grant 2017A030308006, and in part by the High-Level Talents Program of Higher Education of Guangdong Province under Grant 2016ZJ01.

ABSTRACT Recently, IoT has greatly influenced our daily lives through various applications. One of the most promising application is smart city that leverages IoT devices to manage cities without any human intervention. The high possibility of sensing and publishing sensitive data in this smart environment leads to three significant issues: (1) privacy-preserving (2) heterogeneity, and (3) real-time services. We observe that current studies are in lack of addressing these challenges. In this paper, we propose a new privacy-preserving architecture for IoT devices in the smart city by leveraging ontology, a data model, at the edge of the network. At first, we propose an ontology that consists of privacy information of devices. Then, we mount a real-time privacy-preserving method on top of it that is achieved by providing a dynamic environment from the privacy-preserving point of view. Based on the simulation results using Protege and Visual Studio on a synthetic dataset, we find that our solution provides privacy at real-time while addressing heterogeneity issue so that many IoT devices can afford it. Thus, our proposed solution can be widely used for smart cities.

INDEX TERMS Privacy-preserving, ontology, smart city, edge computing, Internet of Things, wireless sensor networks.

I. INTRODUCTION

With the current advancement of wireless sensor networks and machine-to-machine communications, we have entered the IoT era. The aim of IoT is connecting all objects around the world through the Internet [1]. IoT devices are used to contribute to local activities such as monitoring and finding new knowledge about the environment that should be performed without any human intervention [2], [3]. So, we can leverage IoT's great potentials in a variety of domains.

One of IoT's great applications is smart city that has faced with striking advancements with the help of the development of IoT-enabled devices. IoT-based services have to be linked to end devices (e.g., sensors and actuators equipped with processing, storage, and communication capabilities) to provide higher-level services [4]–[6]. Smart city hires IoT with the following aims:

1) Facilitating different domains of its services.
2) Responding to the city community changing needs.
3) Collaborating with other communities if needed.

Actually, these aims are to provide a better use of public resources and services as well as reduce the operation and administration costs.

Fig. 1 explains the concept of the IoT-based smart city from the abstract point of view. As Fig. 1 shows, each part of the smart city such as skyscrapers, smart buildings, smart shops, and smart homes can talk with each other through the Internet, using both unlicensed and licensed frequency bands, to provide more abstract services. Each object shares its data, e.g., current status and data to others to provide better city management. The IoT-based applications may be run

The associate editor coordinating the review of this manuscript and approving it for publication was Junaid Arshad.

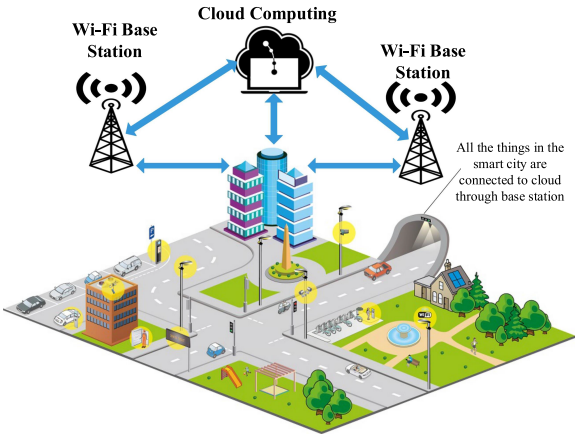

FIGURE 1. Miniature of smart city.

either locally (e.g., lightening systems) or using cloud/edge computing services (e.g., smart transport and intrusion detection services) [6].

On the one hand, IoT devices should have the incompetence to send their data over the network. On the other hand, they produce data over time. Meanwhile, some IoT devices may capture private and disclose sensitive information so that they may cause vulnerability for the system [7]. Private information can be categorized into three main sub-classes as follows:

1) Personal information: Such as Social Security Number or SSN.
2) Sensitive information: Such as salary.
3) Quasi Identifier information: Such as age and zip code. We need to preserve Quasi Identifiers private because we can specify individuals from joining those data with the combination of information that have gained from external sources such as hospitals, fire stations, super markets and so on.

We should keep these three types of data private so that individual's information cannot be revealed without appropriate permission, privacy-preserving. Two major approaches for privacy-preserving are content protection and context protection [8], [9]. Content protection is to protect sensitive data from unauthorized users without appropriate permission. On the contrary, context protection is to keep non-sensed-data of device safe, e.g., time and location of sensing.

We can regard an ontology as a kind of explicit specification of shared conceptualization. Ontology can be used for automatic processing via machines which do not have any perception. According to [10], ontology is one of the key requirements for designing context-aware computing systems because of the following reasons. First, ontology enables the sharing of knowledge among open, dynamic, and distributed systems. Second, ontology along with efficient declarative semantics helps intelligent devices to work out contextual information. Finally, ontology allows agents and devices, which are not originally designed to cooperate, to interoperate so as to achieve *serendipitous interoperability*. To address information leakage and privacy issues, ontology is applicable for dealing with the following challenges:

- Understanding and standardizing the data privacy and/or privacy rule presentations.
- Reusing of data privacy policies.
- Changing the behavior of the system from privacy aspect so that privacy rules of devices become dynamic behaviorally.

By the use of ontology in privacy domain, we are able to control who and which user, IoT device, under what condition, for what aim, and whether he has right to access information or not [11]. Furthermore, we are able to do a semantic interpretation of events and gain an context-aware IoT-based smart city environment that is flexible [12]. A novel architecture with the help of ontology without disclosing sensitive information at the edge of the network has been proposed [13]. However, we are not aware of any existing research work focusing on context-aware privacy preservation for IoT-based smart city.

In this work, the following major issues addressed:

1) A unified privacy rule description because we standardized the use of the presentation of policy rules.
2) A common understanding of the privacy rules among network devices.
3) Reusing of the privacy policies.
4) Changing system behavior from static to dynamic so that attackers can not find acting rules of the system.

This paper is organized as follows. Section II describes related works. Section III describes network model, edge-computing, and problem formulation. Section IV indicates our proposed architecture, namely ECA, its ontology and also its environment. Finally, Section V concludes the paper and also presents possible future works to have a better smart city.

II. RELATED WORKS

Each vendor of IoT devices tends to develop smart devices based on their desires that most likely will end up heterogeneity of produced devices and possibly conflicts between a variety of produced platforms. In addition, the generated data should remain safe so that no one can steal and misuse data. In the following, we summarize some state-of-the-art research works focusing on the security and privacy of IoT applications. Readers are invited to refer to [15] for a survey on ontology for security and privacy challenges in various computing systems and architectures.

In [14], the authors described a new multi-layer cloud architectural model that was developed for interoperability of heterogeneous devices and/or services provided by several vendors in IoT-based smart homes. Furthermore, they used ontology as an alternative tool for knowledge representation to address heterogeneity issues of smart homes. They also proposed a security framework based on the ontology. They proposed the following ontology for security-preserving in smart homes as it is shown in Fig. 2. They used Semantic Web Rule Language (SWRL) to explain the reasoning rules to interoperate on the heterogeneous devices [16].

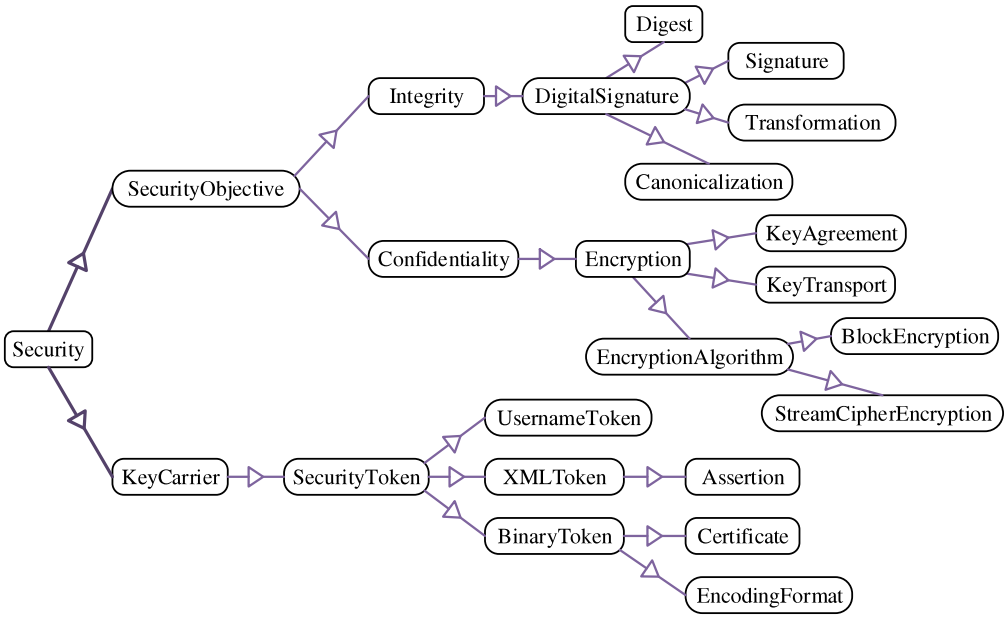

FIGURE 2. Security diagram for our context-aware ontology [14].

Despite several advantages, their system has some disadvantages such as scalability and fault tolerance.

The authors in [17] proposed a novel authentication solution for IoT environment based on identity and SDN paradigm. They also implemented a trusted certificate authority on the SDN controller of SDN architecture. They proposed a security protocol for authentication in order for each device to authenticate by itself. One drawback of their system is that the method was not deployed and evaluated. Thus, there is no performance analysis for their method and their method would not be comparable.

Nobakht *et al.* [18] proposed a framework for intrusion detection in IoT based on SDN paradigm and host. They tried to solve the problem of attacking against a specific host. Authors minimized communication and computation costs by considering only the activity and traffic of a specific node (i.e., the target host). They considered the heterogeneity of network that can be solved with SDN architecture. Their method called IoT-IDM monitors suspicious activities in the network and tries to extract features based on the network flow data. They used machine learning for malicious traffic detection. In detail, they used Support Vector Machine (SVM) for classifying data and detecting abnormal hosts conditions [19]. They also tried to select features of current attack. They used heuristic methods to extract features based on learnt signature patterns of known attacks. They tried to mitigate attack effects by loading required traffic rules on switches and hubs. One of the drawbacks of their method is that feature selection is extracted in a static mode and not dynamically that causes distinguishing malicious flows of all kind of attacks are impossible. Another disadvantage of IoT-IDM is that it can only protect a determined host, not the whole network.

Most existing research works are network-centric, which is opposed to our context-aware scheme. This motivates us to develop a context-aware privacy-preserving scheme for IoT-based smart city. Compared with network-centric approaches, our proposed one is implemented at the network edge through the exploitation of edge computing. Therefore, our proposed approach would utilize great advantages from edge computing concepts, such as, on-premises, proximity, lower latency, location awareness, and network context information (i.e., context awareness) [20].

III. PROBLEM FORMULATION

At first, we have a look at the IoT environment and then formulate the problem and challenge.

A. NETWORK MODEL

Concisely, IoT means connecting machines and devices with each other through the Internet to provide high-level services [21]. Things can be a human to monitor implant, non-human creatures or even any handicrafts that can have a unique identifier or IP. In addition to only gathering information, the data need to be shared with other things such as fire stations, BTSs [22], hospitals, schools to provide quality life [23]. IoT has a great impact on our future life style. If we can address its challenges, we have stronger relish in using this technology. In IoT space, each device disseminates its data in wired or wireless mode to collaborate with other devices to provide a higher level of services with the help of using and analyzing others' data. In all IoT applications, we should not disclose the sensed sensitive data. Devices share their data to use others' data so that we must take more heed to the privacy of produced data [24].

TABLE 1. Comparison between fog computing, multi-access edge computing, and cloudlet computing [25].

	Fog Computing	Mobile-Edge Computing	Cloudlet Computing
Node devices	Routers, Switches, Access Points, Gateways	Servers running in base stations	Data Center in a box
Node location	Varying between End Devices and Cloud	Radio Network Controller/Macro Base Station	Local/Outdoor installation
Software Architecture	Fog Abstraction Layer based	Mobile Orchestrator based	Cloudlet Agent based
Context awareness	Medium	High	Low
Proximity	One or Multiple Hops	One Hop	One Hop
Access Mechanisms	Bluetooth, Wi-Fi, Mobile Networks	Mobile Networks	Wi-Fi
Internode Communication	Supported	Partial	Partial

B. EDGE COMPUTING

Edge computing is an extension of Cloud Computing. In edge computing, servers and carriers are taking pressure off their centralized data centers through edge computing solutions with the help of moving data centers to the edge of the network, closer to data owner [6], [26]. It speeds up the storage processing, data analysis speed without sending them back to a centralized data center that is located in Cloud Computing environment. This leads to better performance, faster average response time. Edge computing plays the role of a broker between IoT devices and cloud computing environment that leads to raising the speed of data analysis. Moreover, edge computing has a relation to the cooperative data centers. Due to the importance and advantages of edge computing compared with cloud computing, moving cloud-computing capability and functionalities to the network edge has been researched extensively over the past decade.

It is worth mentioning that our approach proposed in this work can be implemented with any edge computing paradigm. There have been a number of edge computing concepts, e.g., cloudlet [27], fog computing [28], and multi-access edge computing (MEC) [20]. There exist some similarities and differences between these concepts, as illustrated in Table 1. Let us briefly present two main differences between fog computing and MEC as follows. MEC was developed by European Telecommunications Standards Institute in 2014 while fog computing was introduced by Cisco in 2012. In addition, fog nodes are not integrated into mobile networks, whereas MEC servers are deployed as a part of mobile networks. Therefore, fog computing is usually favored by the service providers and MEC is preferred by telecommunication infrastructure companies. Regardless of the edge computing concept, our approach utilizes the proximity between edge nodes and IoT devices so that data and computations offloaded from IoT devices can be completed within a much lower period of time when compared with traditional cloud computing.

IV. ECA

In this part, we pay our attention to the whole ECA architecture that is based on ontology for privacy-preserving in the IoT-based smart city environment. In fact, at first, a general ontology privacy rule model will be designed by determining the correlative concepts from the privacy-preserving point of view [29]. In next step, we regularly change the privacy rule behavior of the system to convert system behaviour to dynamic mode to have a more efficient privacy-preserving system [30]. The ontology is created by Protege software version 5.2.0. [31].

ECA can be divided into two main sub-classes:

- ECA ontology
- ECA environment

The ECA has three privacy-preserving levels. Thus, attacking system is tougher and comparatively impossible for penetration. Finding original data is described as follows:

- IoT devices, end-users have their own privacy rules.
- Next, a new privacy rule policy is selected randomly.
- The privacy rule behavior of system is changing highly during time.

A. ECA ONTOLOGY

In IoT environment, we are facing with some critical challenges that hinder us to provide efficient IT-supported services such as addressing heterogeneity of devices, services, and data formats that are advanced by their solutions of different vendors [32]. These challenges disturb the prevalence application of IoT. If there is no administration tool, it is possible that these IoT devices provide sensitive information and causes information leakage. In addition, to offer context awareness, we need a high-level knowledge-base that is united with raw sensor data. One tool that can be used for this aim is ontology [33]. In the ontology, we specify privacy knowledge of the domain [34]. In other words, it is one of the most effective means that can be used not only for data demonstration such as privacy rules, but also for solving the heterogeneity issue of provided applications. It demonstrates a high-level of abstraction for addressing privacy objectives [35], [36]. In ECA, we facilitate the knowledge of privacy rules of each device along with its privacy rule lifetime and its owner. It is clear that ECA ontology can be expanded and enhanced by additional privacy terminologies, introducing new classes, associations, and properties. The ontology size of the smart city can be increased. The defined domain ontology model is scalable so that it can be expanded easily.

In traditional systems, there is usually only one static privacy rule for an entire system, i.e., a privacy rule is applied for all the IoT device. Generally, the system is static from the privacy rule point of view. ECA can be defined

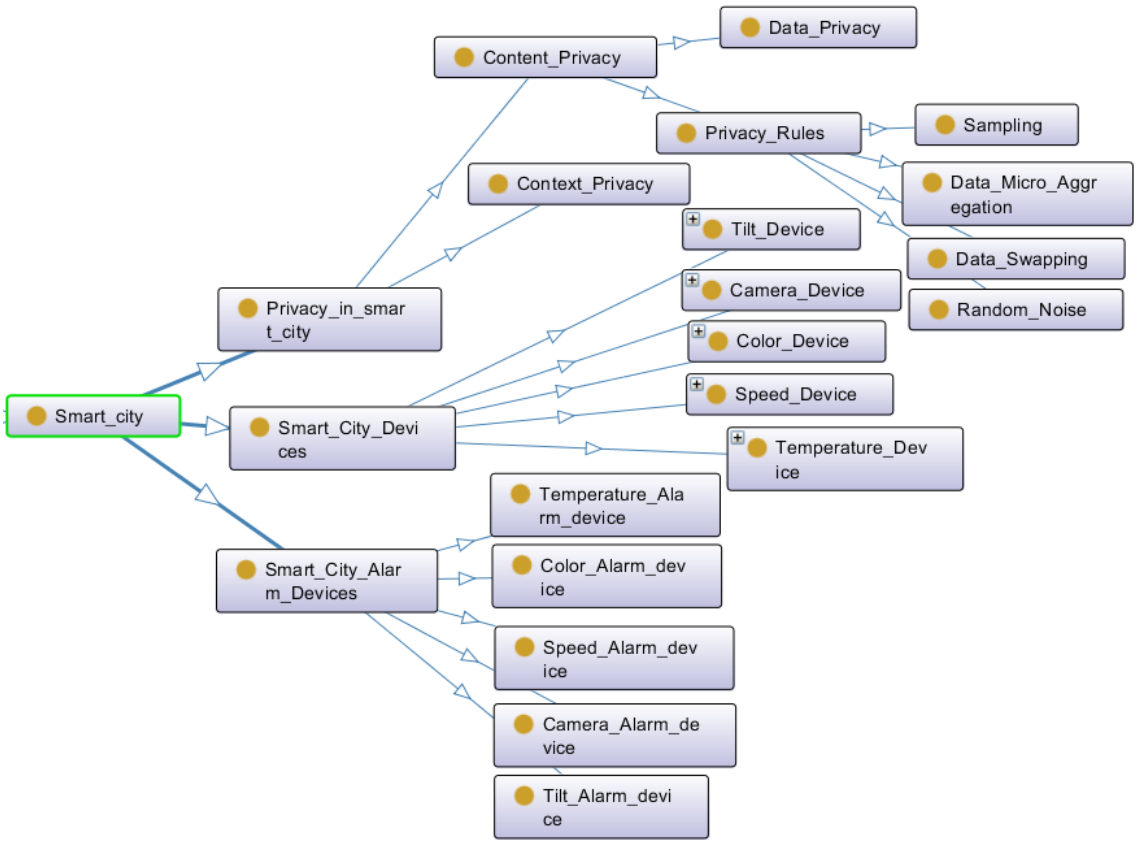

FIGURE 3. Top level structure of privacy rule ontology.

as a supplementary to traditional privacy-preserving methods [37]. That is to say, an IoT-based smart city can apply both the traditional method and ours, in which some IoT devices share the static privacy rules while the remaining ones can select their privacy methods. With the help of ECA, each device has its own privacy rule and the network system converts to dynamic mode so that it is more difficult for attackers to attack the system and find the original data, thus resulting in lower penetration rate. The privacy nature of the system is highly dynamic. In brief, ECA is an ontology-based architecture that converts smart city managing system from static to dynamic mode.

Fig. 3 describes the proposed privacy ontology, is located at the edge of computer for satisfying real-time demands, in the IoT-based smart city environment. Here, smart city class includes smart city devices, smart city alarm devices, and privacy in smart city. The privacy in smart city class indicates the privacy objectives, context privacy and content privacy in the process of interactions or interoperations, which can be gained in the ontology by specifying two sub-classes, Data privacy and Privacy Rules. Privacy Rules class is used to find the next privacy algorithm, e.g., data Swapping [38], random noise data perturbation [39], and data micro aggregation [40]. In [41], three points was proposed for privacy preservation, including privacy noise, plausible deniability, and truthful population. This work motivated us to investigate a privacy-preserving scheme for IoT-based smart cities, where each IoT device can select its own privacy method from the set of three above privacy rules.

Smart city in the developed ontology includes smart city devices, which is divided into five major sub-classes: camera devices, tilt devices, speed devices, temperature devices, and color devices. Camera device class includes five camera instances that are numbered from 1 to 5. Speed class of IoT devices sense speed of the goal objects, record, and report them if any abnormal situation occurs. It consists of two-speed devices called speed sensor and speed sensor 2. Tilt sensor class is in charge of measuring the steep of target objects to provide higher-level and more humanized services with the aim of providing quality life. Temperature IoT devices sense and report the collected temperature values to find irregular conditions such as a possible fire in open areas, forest. And the latest IoT-based smart city device class in our projection is color class that includes two individuals: color sensor and color sensor2. The color class should sense the color of the target objects for example in the smart city environment, color of passing cars on the road for better city management. In the projected ontology, the second level class is linked with the smart city alarm devices. The goal of these classes is when an abnormal condition detected, these classes should be triggered.

TABLE 2. Instances characteristics.

	Device Type	Privacy Method	Privacy Life Time	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 2	Variable Reluctance	3	1	TM
Speed Sensor 2	Intrinsically Safe Speed Sensors ATEX, IECEx, and CSA Certified	2	2	TM
Temperature Sensor 2	Celsius Scale Temperature Sensor	3	2	M
Temperature Sensor 2	NTC thermistor	2	3	M

TABLE 3. The privacy rule approaches and their equivalent numbers.

Privacy Number	Privacy Method
1	Blocking
2	Swapping
3	Random Noise

Concisely, we have twelve IoT devices in smart city that are cameras, speed sensors, temperature sensors, color sensors and tilt ones. Each IoT device has four properties: privacy rule method, privacy rule lifetime, type, and owner. For example, the data type of camera 1 is string and its value is ''Super-Zoom'' as shown in Table 2 [42], the privacy method is 1 that explains blocking method as shown in Table 3, the privacy rule lifetime is 5 (i.e., after 5 time slices, the privacy rule of this IoT device is changed to another privacy rule), and the owner of this camera is traffic manager (TM) of the city [43]. For camera number 2, the privacy method is 3 denoting Random noise technique, the privacy lifetime is 4, the camera data type is string and its value is ''Compact'' [44]. This process is true for all of the smart city devices accordingly.

As Table 3 displays, we have three numbers describing privacy methods. Number 1 specifies that privacy technique of the device is blocking [45]. Number 2 indicates the privacy scheme is data swapping [46], and the last one, number 3, shows the IoT-based smart city device is using Random Noise Method for privacy preserving [39].

B. ECA ENVIRONMENT

After creating ontology that consists of privacy knowledge of IoT devices, we can put our algorithm on top of the smart city environment, which can be illustrated in Alg. 1.

Firstly, each IoT device sends its ID to the ontology server in the edge cloud. When the privacy rule lifetime equals to zero, the owner of the IoT device should be changed. Then the edge server chooses the next proper privacy rule to be applied. We use owner of the device in our ontology to confuse attackers more. Otherwise, the server reduces one from its privacy rule lifetime (line 10). If the life time is greater than zero, the server returns the privacy method back to the IoT device. Then, the IoT device applies its new privacy rule. Finally, the IoT device sends its processed data to the edge cloud and/or to the remote cloud for further analysis. We note that a computation task can be either executed locally by the IoT device or offloaded to one or more edge and remote servers. Furthermore, different computing servers can collaborate to further improve the computing capability at the network edge.

Algorithm 1 The Proposed Context-Aware Ontology-Based Privacy-Preserving Algorithm for IoT-Based Smart Cities

1: **Initialization**: The set of IoT devices $\mathcal{N}$ and initialize the privacy methods at the edge cloud.
2: **Find a suitable privacy rule for each IoT device**
3: **for** Each device $i \in \mathcal{N}$ **do**
4: Ask the ontology in the edge for its life time *ltime*.
5: **if** $ltime = 0$ **then**
6: Change the owner of the IoT device.
7: Find the next privacy rule
8: Apply the new privacy rule for the IoT device.
9: **else if then**
10: Reduce the life time by 1, i.e., $ltime = ltime - 1$.
11: Return the privacy rule.
12: Apply the returned privacy rule.
13: **end if**
14: **end for**
15: Each IoT device send its processed data to the cloud.
16: **End of the algorithm**: Privacy rule of each IoT device.

Cloud is an infrastructure that supports IoT infrastructure to achieve better performance. It has some capabilities that are unlimited scaling, elasticity and using shared services [47]. One of the major benefits of Cloud is virtualization; it can help IoT environment to increase the limited computing and storage capabilities because most of IoT devices are resource-constrained [26], [48]. It is notable to mention that leveraging Cloud Computing particularly Edge-computing with IoT is in its infancy stage in the smart city application and most of the proposed solutions have not fully used the benefits of these great technologies. The advantage of ECA is that if an external attacker wants to find the original data, at first it needs to find privacy rule of victim device. However, because the system is dynamic, it would be more difficult for the attacker to find the original data.

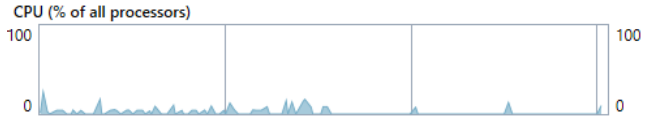

FIGURE 4. Computational cost.

We simulate the proposed framework environment, ECA, with the help of Visual Studio.net 2015 and Protege. For ontology part of ECA, Protege version, 5.0.2 and its plugins are used. To simulate the environment, we use Visual Studio.net, CSharp.net, as a simulator of the smart city. For simplicity, we consider each individual, i.e., IoT device, as a bulb and denote each privacy rule as its color. We have three privacy rules, each of which is represented by a number. In particular, blocking, swapping, and random noise are denoted by 1, 2, and 3, respectively (c.f., Tables 3 and 2). Each device has its own privacy rule lifetime that describes how much time the privacy rule is valid. Each time slice, lifetime should be deducted. If the server finds that the lifetime is zero, it should change the privacy rule of the device and its owner, changing its color.

But from the coding aspect, each device has a cycle that displays its privacy past time. In the beginning, when each device begins, all bulbs are off. Next, the server allocates each device its privacy method and its privacy rule lifetime. The server continuously checks the device's privacy rule lifetime each cycle. If any privacy rule lifetime of devices becomes zero, the server changes the owner and then selects new privacy rule, color, at random and assigns the selected value to the device. Then, the device applies the new privacy method. Meanwhile, each IoT device gathers generated data and sends them to the edge for further process and real-time analysis.

For evaluation of ECA, we calculate the amount of CPU overload to the system. Fig. 4 shows the CPU usage of all devices through time. It is obvious that the amount of the computational cost of the system is less than 10 percent that shows the ECA is applicable to most of the application. But preferably more suitable for IoT devices that are not resource-constraint.

V. CONCLUSION AND FUTURE WORK

With the emerging technology advances such as IoT that has supported the growth of the smart city applications, each IoT device in smart city universe yields increasing data over time. These data can be sent to the edge of the network for further analyses and satisfying real-time services. If we do not control produced data, it may lead to disclosing sensitive information and information leakage. Ontology can be applied as an encouraging tool to solve many challenges such as standardization, heterogeneity issue, interoperability and so on. In this paper, we have modeled an architecture for privacy-preserving called ECA at the edge of the network that is based on the ontology in order for system to convert to highly dynamic mode in privacy behavior aspect. ECA provides three layers of privacy protection. Many possible future works can be done such as finding the best privacy rule based on logic, taking into consideration the penetration rate of the system and accuracy of the architecture, and comparing ECA with other proposed methods through more possible parameters such as accuracy.

ACKNOWLEDGMENT

National Natural Science Foundation of China under 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.

REFERENCES

[1] M. Gheisari and M. Esnaashari, "Data storages in wireless sensor networks to deal with disaster management," in *Proc. Emergency Disaster Manage., Concepts, Methodol.*, 2018, pp. 196–222.
[2] H. K. Patil and T. M. Chen, "Wireless sensor network security: The Internet of Things," in *Computer and Information Security Handbook*, J. R. Vacca, Ed., 3rd ed. Boston, MA, USA: Morgan Kaufmann, 2017, pp. 317–337.
[3] S.-H. Yang, *Internet of Things*. London, U.K.: Springer, 2014, pp. 247–261.
[4] M. Gheisari, "Design, implementation and evaluation of SemHD: A new semantic hierarchical sensor data storage," *Indian J. Innov. Develop.*, vol. 1, no. 3, pp. 115–120, Mar. 2012.
[5] M. Gheisari, A. A. Movassagh, Y. Qin, J. Yong, X. Tao, J. Zhang, and H. Shen, "NSSSD: A new semantic hierarchical storage for sensor data," in *Proc. IEEE 20th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, Nanchang, China, May 2016, pp. 174–179.
[6] Q.-V. Pham, F. Fang, V. N. Ha, M. Le, Z. Ding, L. B. Le, and W.-J. Hwang, "A survey of multi-access edge computing in 5G and beyond: Fundamentals, technology integration, and state-of-the-art," 2019, *arXiv:1906.08452*. [Online]. Available: https://arxiv.org/abs/1906.08452
[7] C.-Z. Gao, Q. Cheng, X. Li, and S.-B. Xia, "Cloud-assisted privacy-preserving profile-matching scheme under multiple keys in mobile social network," *Cluster Comput.*, vol. 22, pp. 1–9, Feb. 2018.
[8] Y. Wand, V. C. Storey, and R. Weber, "An ontological analysis of the relationship construct in conceptual modeling," *ACM Trans. Database Syst.*, vol. 24, no. 4, pp. 494–528, Dec. 1999.
[9] T. Peng, Q. Liu, D. Meng, and G. Wang, "Collaborative trajectory privacy preserving scheme in location-based services," *Inf. Sci.*, vol. 387, pp. 165–179, May 2017.
[10] H. Chen, T. Finin, and A. Joshi, "An ontology for context-aware pervasive computing environments," *Knowl. Eng. Rev.*, vol. 18, no. 3, pp. 197–207, Sep. 2003.
[11] M. Peleg, D. Beimel, D. Dori, and Y. Denekamp, "Situation-based access control: Privacy management via modeling of patient data access scenarios," *J. Biomed. Inform.*, vol. 41, no. 6, pp. 1028–1040, Dec. 2008.
[12] A. I. Maarala, X. Su, and J. Riekki, "Semantic reasoning for context-aware Internet of Things applications," *IEEE Internet Things J.*, vol. 4, no. 2, pp. 461–473, Apr. 2017.
[13] H. Suguri, E. Kodama, M. Miyazaki, and I. Kaji, "Assuring interoperability between heterogeneous multi-agent systems with a gateway agent," in *Proc. 7th IEEE Int. Symp. High Assurance Syst. Eng.*, Tokyo, Japan, Oct. 2002, pp. 167–170.
[14] M. Tao, J. Zuo, Z. Liu, A. Castiglione, and F. Palmieri, "Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes," *Future Gener. Comput. Syst.*, vol. 78, pp. 1040–1051, Jan. 2018.
[15] S. Sengupta, J. Garcia, and X. Masip-Bruin, "A literature survey on ontology of different computing platforms in smart environments," 2018, *arXiv:1803.00087*. [Online]. Available: https://arxiv.org/abs/1803.00087
[16] M. O'Connor, H. Knublauch, S. Tu, and M. Musen, "Writing rules for the semantic Web using SWRL and jess," in *Proc. Protégé Rules WS*, Madrid, Spain, Jul. 2005, pp. 1–8.
[17] O. Salman, S. Abdallah, I. H. Elhajj, A. Chehab, and A. Kayssi, "Identity-based authentication scheme for the Internet of Things," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Messina, Italy, Jun. 2016, pp. 1109–1111.

[18] M. Nobakht, V. Sivaraman, and R. Boreli, "A host-based intrusion detection and mitigation framework for smart home IoT using openflow," in *Proc. 11th Int. Conf. Availability, Rel. Secur. (ARES)*, Salzburg, Austria, Aug./Sep. 2016, pp. 147–156.
[19] M. Gheisari, D. Panwar, P. Tomar, H. Harsh, X. Zhang, A. Solanki, A. Nayyar, and J. A. Alzubi, "An optimization model for software quality prediction with case study analysis using MATLAB," *IEEE Access*, vol. 7, pp. 85123–85138, 2019.
[20] Q.-V. Pham, L. B. Le, S.-H. Chung, and W.-J. Hwang, "Mobile edge computing with wireless backhaul: Joint task offloading and resource allocation," *IEEE Access*, vol. 7, pp. 16444–16459, 2019.
[21] L. Atzori, A. Iera, and G. Morabito, "The Internet of Things: A survey," *Comput. Netw.*, vol. 54, no. 15, pp. 2787–2805, Oct. 2010.
[22] M. Gheisari, J. Alzubi, X. Zhang, U. Kose, and J. A. M. Saucedo, "A new algorithm for optimization of quality of service in peer to peer wireless mesh networks," *Wireless Netw.*, pp. 1–9, Mar. 2019.
[23] J. Sethuraman, R. Manikandan, M. Gheisari, A. Kumar, and J. A. Alzubi, "Eccentric methodology with optimization to unearth hidden facts of search engine result pages," *Recent Patents Comput. Sci.*, vol. 12, no. 2, pp. 110–119, 2019.
[24] M. Gheisari, G. Wang, and M. Z. A. Bhuiyan, "A survey on deep learning in big data," in *Proc. IEEE Int. Conf. Comput. Sci. Eng. (CSE), IEEE Int. Conf. Embedded Ubiquitous Comput. (EUC)*, Guangzhou, China, vol. 2, Jul. 2017, pp. 173–180.
[25] K. Dolui and S. K. Datta, "Comparison of edge computing implementations: Fog computing, cloudlet and mobile edge computing," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6.
[26] Q.-V. Pham, T. Leanh, N. H. Tran, B. J. Park, and C. S. Hong, "Decentralized computation offloading and resource allocation for mobile-edge computing: A matching game approach," *IEEE Access*, vol. 6, pp. 75868–75885, 2018.
[27] M. Satyanarayanan, P. Bahl, R. Caceres, and N. Davies, "The case for VM-based cloudlets in mobile computing," *IEEE Pervasive Comput.*, vol. 8, no. 4, pp. 14–23, Oct. 2009.
[28] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, Ottawa, ON, Canada, May 2015, pp. 1202–1207.
[29] M. Alirezaie, J. Renoux, U. Köckemann, A. Kristoffersson, L. Karlsson, E. Blomqvist, N. Tsiftes, T. Voigt, and A. Loutfi, "An ontology-based context-aware system for smart homes: E-care@home," *Sensors*, vol. 17, no. 7, p. 1586, Jul. 2017.
[30] A. Salentinig and P. Gamba, "2.07—Data- and decision-level fusion for classification," in *Comprehensive Remote Sensing*, S. Liang, Ed. New York, NY, USA: Oxford, 2018, pp. 134–155.
[31] J. H. Gennari, M. A. Musen, R. W. Fergerson, W. E. Grosso, M. Crubézy, H. Eriksson, N. F. Noy, and S. W. Tu, "The evolution of protégé: An environment for knowledge-based systems development," *Int. J. Hum.-Comput. Stud.*, vol. 58, no. 1, pp. 89–123, Jan. 2003.
[32] Q. Liu, G. Wang, F. Li, S. Yang, and J. Wu, "Preserving privacy with probabilistic indistinguishability in weighted social networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 28, no. 5, pp. 1417–1429, May 2017.
[33] S. Bechhofer, "OWL: Web ontology language," in *Encyclopedia Database System*. Boston, MA, USA: Springer, 2009, pp. 2008–2009.
[34] M. Tao, K. Ota, and M. Dong, "Ontology-based data semantic management and application in IoT- and cloud-enabled smart homes," *Future Gener. Comput. Syst.*, vol. 76, pp. 528–539, Nov. 2017.
[35] M. M. Rathore, A. Ahmad, A. Paul, and S. Rho, "Urban planning and building smart cities based on the Internet of Things using big data analytics," *Comput. Netw.*, vol. 101, no. 4, pp. 63–80, Jun. 2016.
[36] G. De Giacomo, D. Lembo, M. Lenzerini, A. Poggi, and R. Rosati, *Using Ontologies for Semantic Data Integration*. Cham, Switzerland: Springer, 2018, pp. 187–202.
[37] D. Sánchez, M. Batet, S. Martínez, and J. Domingo-Ferrer, "Semantic variance: An intuitive measure for ontology accuracy evaluation," *Eng. Appl. Artif. Intell.*, vol. 39, pp. 89–99, Mar. 2015.
[38] N. Nethravathi, V. J. Desai, P. D. Shenoy, M. Indiramma, and K. Venugopal, "A brief survey on privacy preserving data mining techniques," *Data Mining Knowl. Eng.*, vol. 8, no. 9, pp. 267–273, 2016.
[39] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," in *Proc. 3rd IEEE Int. Conf. Data Mining*, Melbourne, FL, USA, Nov. 2003, pp. 99–106.
[40] A. Solanas, F. Sebé, and J. Domingo-Ferrer, "Micro-aggregation-based heuristics for p-sensitive k-anonymity: One step beyond," in *Proc. Int. Workshop Privacy Anonymity Inf. Soc.*, Nantes, France, Mar. 2008, pp. 61–69.
[41] J. Joy and M. Gerla, "Differential privacy by sampling," 2017, *arXiv:1708.01884*. [Online]. Available: https://arxiv.org/abs/1708.01884
[42] D. Johnson, *Digital Camera*. New York, NY, USA: McGraw-Hill, 2003.
[43] H. Ebadi, T. Antignac, and D. Sands, "Sampling and partitioning for differential privacy," in *Proc. 14th Annu. Conf. Privacy, Secur. Trust (PST)*, Auckland, New Zealand, Dec. 2016, pp. 664–673.
[44] M. Gheisari, G. Wang, W. Z. Khan, and C. Fernández-Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Secur.*, vol. 87, Nov. 2019, Art. no. 101470. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167404818313336
[45] C. C. Aggarwal and P. S. Yu, "A general survey of privacy-preserving data mining models and algorithms," in *Privacy-Preserving Data Mining*. Boston, MA, USA: Springer, 2008.
[46] V. Estivill-Castro and L. Brankovic, "Data swapping: Balancing privacy against precision in mining for logic rules," in *DataWarehousing and Knowledge Discovery*, Berlin, Germany: Springer, 1999.
[47] C. Stergiou and K. E. Psannis, "Recent advances delivered by mobile cloud computing and Internet of Things for big data applications: A survey," *Int. J. Netw. Manage.*, vol. 27, no. 3, May/Jun. 2017, Art. no. e1930.
[48] A. Botta, W. Donato, V. Persico, and A. Pescapé, "Integration of cloud computing and Internet of Things: A survey," *Future Generat. Comput. Syst.*, vol. 56, pp. 684–700, Mar. 2016.