IEEE Open Journal of Vehicular Technology

Received 28 January 2023; accepted 29 January 2023. Date of publication 8 February 2023;
date of current version 1 March 2023. The review of this article was coordinated by Editor Lina Mohjazi.

Digital Object Identifier 10.1109/OJVT.2023.3243226

An Agile Privacy-Preservation Solution for IoT-Based Smart City Using Different Distributions

MEHDI GHEISARI [1,2], EHSAN SHOJAEIAN [3], AMIR JAVADPOUR [2], AHMAD JALILI [4], HAMID ESMAEILI-NAJAFABADI [5], BAHRAM SADEGHI BIGHAM [6,7], ALISA A VOROBEVA [8], YANG LIU [2], AND MOHAMMAD REZAEI [9]

[1]Department of Cognitive Computing, Institute of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Sciences, Chennai 602105, India
[2]School of Computer Science, Harbin Institute of Technology (Shenzhen), Shenzhen 518055, China
[3]Department of Computer Engineering, Science and Research Branch, Islamic Azad University, Tehran 14778-93855, Iran
[4]Department of Computer Engineering, Gonbad Kavous University, Golestan 4971799151, Iran
[5]Department of Electrical and Software Engineering, University of Calgary T2N 1N4, Canada
[6]Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences, Zanjan 45137-66731, Iran
[7]Department of Computer Science, Faculty of Mathematical Sciences, Alzahra University, Tehran 1993893973, Iran
[8]School of Secure Information Technologies ITMO University, 197101 St. Petersburg, Russia
[9]Department of Advanced Safety and User Experience, Troy, MI 48098 USA

CORRESPONDING AUTHOR: YANG LIU (e-mail: liu.yang@hit.edu.cn).

This work was supported in part by the Shenzhen Basic Research (General Project) under Grant JCYJ20190806142601687 and in part by Shenzhen Stable Supporting Program (General Project) under Grant GXWD20201230155427003-20200821160539001.

ABSTRACT In today's world, everything is connected via the Internet. Smart cities are one application of the Internet of Things (IoT) that is aimed at making city management more efficient and effective. However, IoT devices within a smart city may collect sensitive information. Protecting sensitive information requires maintaining privacy. Existing smart city solutions have been shown not to offer effective privacy protection. We propose a novel continuous method called Differential Privacy-Preserving Smart City (DPSmartCity). When the IoT device produces sensitive data, it applies differential privacy techniques as a privacy-preserving method that uses Laplace distributions or exponential distributions. The controller receives the perturbed data and forwards it to the SDN. SDN controllers eventually send the data to the cloud for further analysis. Accordingly, if the data is not sensitive, it is directly uploaded to the cloud. In this way, DPSmartCity provides a dynamic environment from the point of view of privacy preservation. As a result, adversaries are unable to easily compromise the privacy of the devices. The solution incurs at most 10-18% overhead on IoT devices. Our solution can therefore be used for IoT devices that are capable of handling this overhead.

INDEX TERMS IoT, privacy-preservation, differential privacy, distribution, SDN.

I. INTRODUCTION

It is possible to connect everything, anywhere, anytime via the Internet in order to provide higher-level services and extract useful information from data generated by the Internet of Things (IoT). According to the forecasts and Gartner, the number of devices reached 20 billion in 2020 [1], [2]. The global population is estimated to reach 50 billion by 2050. With such a large population in cities, it is impossible to manage them manually.

With the advancement of wireless sensor networks and machine-to-machine (M2M) communications, the age of the IoT has dawned. The IoT aims to connect all things around the globe, digital or non-digital devices, via the Internet. These IoT devices work together to provide high-value services. Because of the rapid population growth in cities, we can no longer manage their challenges manually, such as the public transportation system. Therefore, innovative thinking and new technologies are vital to handle these challenges

automatically. A promising technology that can help is the IoT.

IoT devices can create a city that can be managed automatically and smartly while improving user experience [15]. For instance, an interconnected infrastructure connecting electric and hybrid electric smart vehicles can significantly improve the driving experience, quality, vehicle safety, and fuel consumption. By using vehicle connectivity features, equipped vehicles with IoT can communicate to receive the latest traffic, surrounding information, and location on their path. Using this information, vehicles can calculate the most fuel economic path and take that path to consume less fuel. The term "smart city" was coined for this purpose. In this light, smart cities try to manage the challenges of cities automatically, even as the population of cities increases.

A smart city is one of the extensive applications of IoT devices. It is an IoT-based city that uses information and communication technologies (ICTs) to increase operational efficiency, share information with the public, simplify city management, and improve both the quality of government services and the well-being of citizens [3], [4], [5]. In addition, smart city devices generate huge amounts of data, including sensitive data. For an autonomous vehicle, such data can be related to its safety and connectivity features or its fuel consumption.

Three types of data should be protected from unintended disclosure:

1) Personal data, such as name, identifier, social security number of sensitive people or safety-related data in autonomous vehicles;
2) Semi-sensitive data, such as salary and diseases;
3) Quasi-identification data, such as age and zip code.

The quasi-identifier refers to the sensitive data because it can identify individuals if it is combined with information from external sources, such as public voter registration data or hospital registration records; thus, we can re-identify individuals through published data [6].

The way sensitive information is disseminated has received much attention in recent years. This data should not be shared because it can lead to security breaches and system damage. There are two key obstacles in privacy protection in IoT-based systems: 1) a large number of connected devices and 2) the use of a traditional network architecture model. Because of the first obstacle, we cannot manually manage all the data published by the devices. Therefore, novel innovative solutions are needed to automatically prevent the disclosure of sensitive data while maintaining the IoT devices' performance. One of the promising methods to address this challenge is Differential Privacy (DP) [7].

In the traditional network architecture model, which is commonly used today, each device is connected to a switch to share its data with others to provide high-level services, indicating that the data and control planes are integrated. This traditional model has significant drawbacks, such as difficult and costly switch upgrades and network management.

Software-Defined Networking (SDN) is a recently emerged trend that provides a flexible network for efficient configuration and management through software [4], [8]. The SDN technology improves network performance and monitoring. Based on DP and SDN concepts, we propose a novel method to ensure the privacy of the smart city, called Differential Privacy-Preserving Smart City (DPSmartCity). It operates as an IoT platform in a smart city that provides privacy-preserving methods. The primary novelty of the proposed method lies in using SDN architecture in combination with DP. In this light, a smart city environment based on IoT-based smart cities is first integrated with SDN network patterns. Then, we mounted a privacy-preserving solution to effectively preserve the privacy of devices. Finally, we evaluate our solution using several evaluation metrics such as mathematical proof.

The structure of the paper is described as follows. Section II describes the background of the study. Section III discusses the related works and shortcomings of the existing solutions. Section IV explains DPSmartCity in detail, mainly consisting of two subparts: facilitating the smart city environment with the SDN paradigm and proposing a privacy-friendly method to prevent information leakage from IoT devices that produce sensitive data. We present our privacy-friendly solution for IoT-based smart city environments. In Section V, we describe the experimental studies and the achieved results. We also present some future work that can be done for a more efficient smart city. Lastly, Section VI concludes the paper.

II. BACKGROUND

A. PRIVACY-PRESERVING IN IOT-BASED SMART CITY

IoT devices produce vast amounts of data over time. Providing high-level services requires sharing these data. A practical example is IoT-based velocity prediction in autonomous vehicles. It significantly improves accuracy in the prediction of vehicle velocity, which can optimize energy management in electric and hybrid electric vehicles. However, the optimization algorithms mostly require heavy computations, which is often not feasible on an onboard electric control unit in the vehicle. Modern vehicles can communicate wirelessly to transmit real-time data about traffic, their surroundings, and their locations. Here, IoT infrastructure plays an important role in the vehicles communication. It essentially facilitates choosing the most economical routes for vehicles to reduce fuel consumption. The generated data, including safety and energy management, is often transmitted over wireless networks. Therefore, establishing privacy-aware methods to protect this data is of utmost importance.

When IoT devices collect sensitive data, sharing and exchanging them can become a critical issue. It is possible that third parties may misuse the generated data and harm the system because of system vulnerabilities. Privacy preservation refers to preventing such misuse. By resolving the privacy-preserving problem, more people will trust IoT-based smart city environments.

In this light, we focus on the privacy-preserving problem of IoT devices in the smart city environment and the data, the disclosure of which may lead to system vulnerabilities and damages.

B. SOFTWARE-DEFINED NETWORKING (SDN)

In the traditional networking paradigm, every device is connected to a switch. Switches often get crowded. To resolve this, most modern systems include a costly, fully integrated package of hardware, operating systems, and applications. In such a system, the data plane is mixed with the control plane, which leads to various problems, such as being unable to control data flow.

Moreover, network maintenance is a very tedious task because updating switches and manipulating them requires manual work. It is time-consuming, tedious, and prone to human error. All these challenges arise from the fact that the control plane and the data plane are mixed.

To overcome the above challenges, SDN [5], [18] attempts to bring flexibility to the network by separating the data and control planes. In this case, switches are dumb with a small amount of programmability, mostly OpenFlow [5], [17]. This separation allows us to control the network through software.

In the SDN domain, SDN controllers control the data flow from the switches. Centralized control provides the ability to manage the network remotely. However, the problem of single-point failure occurs.

III. RELATED WORK

Only a few works have addressed the privacy-preserving aspects of smart cities. Therefore, we focus on the related outcomes that try to preserve the privacy of IoT devices in the smart city environment.

In [9], the authors presented a privacy-preserving method based on modular arithmetic when IoT devices generate sensitive timestamps. This work presents a privacy-preserving algorithm that hides the IoT device's time. A possible privacy-preserving solution is allowing each device to apply privacy-preserving algorithms to protect the privacy and perform analytics.

The authors in [10] proposed a privacy-preserving method for wearable devices, which are an application of IoT. Personal data was collected through wearable devices. It is important to share this data with others so that they can benefit from it. Because of this, a threat model based on a linkage attack on wearable devices was first proposed. Then, a privacy-preserving method based on clustering known as k-anonymity is proposed.

The authors in [11] proposed a framework to address the problem of heterogeneity and privacy protection of IoT devices at the network edge using a novel ontology data model.

In [12], the authors proposed a lightweight privacy-preserving data aggregation (LPDA) method for fog computing-enhanced IoT. They used homomorphic Paillier encryption to encrypt the data. They also applied the Chinese Remainder Theorem for the hybrid aggregation of multiple different IoT devices. Moreover, they used one-way hash chain functions to filter out false data in the network edge and authenticate IoT devices. Differential privacy-preserving techniques are shown to improve the privacy of LPDA [13].

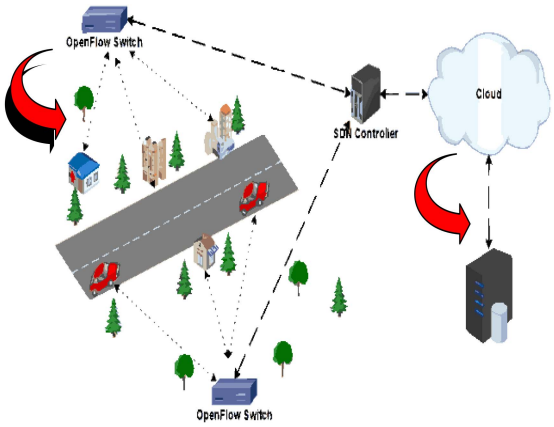

FIGURE 1. Equipped iot-based smart city with SDN paradigm.

Meanwhile, the research trend went towards using the SDN paradigm with the IoT-based smart city environment, as presented by the authors in [14], [22], [23], [24]. They first simplified the IoT environment with the SDN paradigm. They also proposed a privacy-preserving method for IoT devices that produce sensitive data.

The authors of [16] presented an efficient method for privacy-preserving in a smart city supported by the SDN paradigm [17], [18], [19], [20], [21], [22]. First, the IoT-based smart city is equipped with the SDN paradigm. Then, a method is proposed to protect the privacy of all kinds of IoT devices with different degrees of privacy. This is achieved by the SDN controller, which manages the data packets of all IoT devices and divides their data according to the context.

The previous methods and their features have been summarized in Table 1.

IV. DIFFERENTIAL PRIVACY-PRESERVING SMART CITY METHOD AND PROPOSED MODEL

Here, we introduce an SDN-based solution in the environment that can preserve privacy and bring flexibility to network management, DPSmartCity.

The main idea of the proposed method is revealed in the following pseudo-code.

To address the existing shortcomings of related works, we propose the DPSmartCity method, which aims to create an efficient IoT-based smart city. It is the IoT platform in a smart city that provides privacy-preserving methods. DPSmartCity method consists of two parts:

1) An IoT-based smart city equipped with the SDN paradigm, i in Fig. 1.
2) A Method for the equipped smart city that preserves the privacy of IoT devices with DP.

TABLE 1. Comparison Between Related Works

Method	Adopted solution	Advantages	Disadvantages
A Modular Arithmetic Algorithm for Privacy Preserving in IoT [9]	- Number Theory - Modular Arithmetic	The energy consumption	**Its scalability and overhead are not given.**
A Clustering-Anonymity Privacy-Preserving Method for Wearable IoT Devices [10]	Clustering k-anonymity	The most secure method of the four methods considered.	**The process is performed on the server-side.**
An Edge Computing-Enhanced Internet of Things Framework for Privacy-Preserving in Smart City [11]	Ontology data model	The number of devices is not taken into account.	**It is a cost-effective method for many IoT devices that are not very limited in terms of resources.**
A Lightweight Privacy-Preserving Data Aggregation (LPDA) Method [12]	- Homomorphic paillier encryption - Chinese Remainder Theorem - One-way hash chain functions - Differential privacy-preserving techniques [13]	- The solution is secure while improving privacy. - Their system is lightweight.	**- Their system is not flexible and nimble. - Updating the fog nodes has to be done manually.**
A Method for Privacy-Preserving in IoT-SDN Integration Environment [14]	Each device has different privacy rules for each snapshot.	It brings flexibility into the environment.	**- The degree of privacy preservation has not been calculated. - The complicated decision of the SDN controller**
A Context-Aware Privacy-Preserving Method for IoT-Based Smart City Using SDN Paradigm [16]	**Each device splits its data into two parts based on the command received from the SDN.**	**- No loss of sensitive information -It can be widely deployed for smart city applications.**	**It is an inappropriate solution for devices with limited resources.**

The advantages of the SDN architecture have been described in detail above. Therefore, the SDN network paradigm can affect highly dynamic environments, such as smart cities.

Fig. 1 demonstrates that each IoT device is connected to an OpenFlow switch. And they, in turn, are connected to an SDN controller. And the SDN controller has a reciprocal relationship with the cloud computing domain. Our smart city scenario uses SDN to connect IoT devices to each other and send their data to OpenFlow switches. These switches are then connected to the SDN controller via wired or wireless connections. The SDN controller controls and manages these switches. The SDN controller is also connected to the

Algorithm 1: Privacy Preserving in the Proposed Method.

Input: *Distribution function, Data generated, Timer*
Output: *Conversion data*
Get data generated and distribution function
if ***the*** *data generated is sensitive,* **then**
  if *timer = 60* **then**
    if *distribution function = Laplace* **then**
      Distribution function ← Laplace
    end
  end
  else
    Differential privacy is applied to IoT devices using distribution function
  end
  Output the conversion data and send it to the cloud
end
else
  The data generated are sent to the cloud directly
end

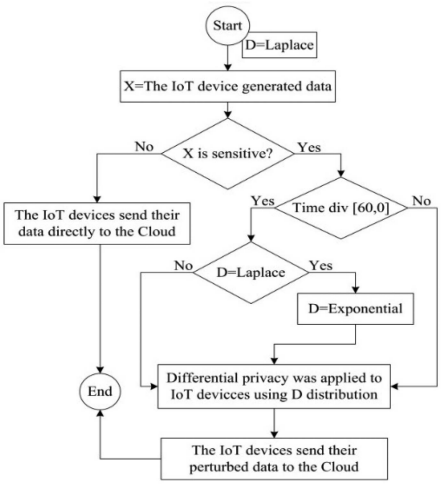

FIGURE 2. The details of flowchart privacy-preserving on top of the equipped IoT-based smart city.

Cloud environment, as depicted in Fig. 1. With this smart city architecture, we can leverage the advantages of SDN architecture (e.g., flexibility, remote management, and centralized management). At the same time, the privacy of data is preserved. The SDN controller has two mutual connections to the Cloud environment. It denotes that the SDN controller can get commands from the cloud environment and pose them to IoT devices, a mutual relation.

In this light, we first deal with the IoT-based smart city equipped with the SDN paradigm and then the built-in privacy-preserving method.

The flowchart of the proposed privacy-preserving method based on the equipped IoT-based smart city of the DPSmartCity method is depicted in Fig. 2.

The controller receives the perturbed data and then sends it to the SDN. Eventually, the data is sent to the cloud for further analysis by the SDN controller.

TABLE 2. Units for Magnetic Properties

Protocol number	Probability of initial failure of the protocol in constant time M
1	p_1
2	p_2
3	p_3
4	p_4

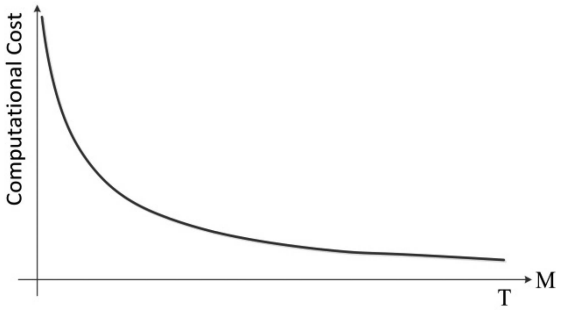

FIGURE 3. The relation between computational cost and T.

However, the IoT device sends directly to the cloud if the data are not sensitive.

When the IoT device produces sensitive data, it applies DP as a privacy-preserving method. Specifically, each IoT device in the smart city environment has two ways to choose its privacy-preserving method:

1) Differential privacy-preserving method with Laplace distribution;
2) Differential privacy-preserving method with exponential distribution.

The SDN controller changes the distribution of applied DP every minute. That is, sensitive IoT devices' distribution of the applied DP method changes every minute and fluctuates between Laplace distribution and exponential distribution. After using one of the two DP methods, the device sends its data directly to the cloud.

Since the selected privacy-preserving method of each IoT device changes every minute, the dynamic of the environment and the hard intrusion of DP prevent the disclosure of sensitive data more effectively. The proposed method can be formulated as follows.

Let's assume data is exchanged between IoT devices and receivers as quickly as possible. However, sometimes it takes hours to send data. Whenever the transmission of information exceeds the *M* time intervals, the protocol changes, and we use the other method in the middle of sending. Therefore, if t_i is the time required to send a message, we consider the validity period of the selected protocol equal to $\tau_i = \min\{t_i,\ M\}$.

Suppose the probability of breaking the security of the protocols in a fixed period M is as given in Table 2.

Obviously, p_i has a direct relationship with the M, and the larger the value of M, the more likely the protocol will fail. Accordingly, p_i would be 1 when the M value tends to ∞. Instead ∞, we consider the T symbol as a long time in which all protocols can be definitively broken. Therefore, by setting M, we get to the following formula:

$$p'_i = p_i + \left(1 - p_i * log_T^M\right). \tag{1}$$

If M is valued as T, the p'_i will be equal to 1, indicating a definitive failure of the protocol in a long time T.

Another part of the job is to make hacking more difficult. It is the choice of protocol at the start of the attack that reduces the probability of success to 1/4. Therefore, if p is the probability of success at any moment (regardless of the specific method) the probability of success can be equal to 1/4 the expected value of the other four methods:

$$p = \frac{1}{4}\left\{\frac{\sum p'_i}{4}\right\} = \frac{\sum p'_i}{16} \tag{2}$$

According to the above, the computational complexity of the proposed algorithm can be shown as follows:

This computational cost directly results from the number of processes involved. In addition, if we consider p' as the probability of failure of the whole algorithm, p' has a minimum value for small values M, and when M is equal to T value, its maximum value reaches 1.

By implementing the method for different M modes, the best situation can be obtained in the tradeoff between the computational cost criteria and the probability of failure of the whole algorithm.

V. SIMULATION AND EVALUATION

IoT devices are known for having limited computational capacities. The overhead is the most important issue at this stage of research that should be studied experimentally. In this section, we evaluate our solution based on the overhead to find out how much pressure our solution puts on IoT devices.

The overhead is the percent of average extra CPU usage spent by the devices on which the DPSmartCity method was implemented. The general simulation details and the overhead incurred are discussed below.

We integrated the SDN paradigm with the smart city domain. Because of the smart city being a highly dynamic environment, we gained many advantages by using SDN. We simulated our method with the help of C#, benefiting from the visual studio.Net, version 2018.

In the simulation, we increased the number of sensors in the IoT from 175 to 250, and the changes in processing rates are reported in Fig. 3 .

The average CPU usage of the entire network is shown in Fig. 3. For simplicity, we depict CPU usage results only for four states, but the trend is similar to the others. As observed, the CPU usage during execution almost fluctuates across the different executions. For instance, the CPU usage for 250 devices is 23%, 21%, and 24% in times of 1, 4, and 14 (s), respectively. Meanwhile, the overhead for 175 devices is 16%, 11%, and 16% in time 1, 4, and 14 (s), respectively.

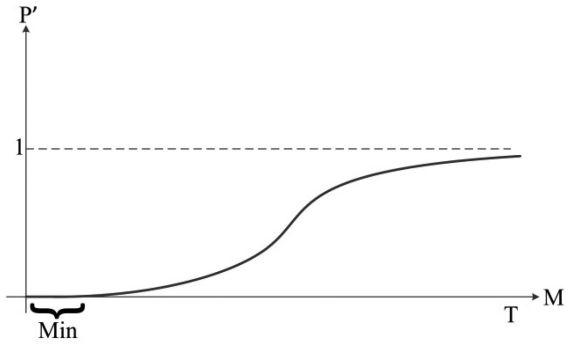

FIGURE 4. The relation between total probability and T.

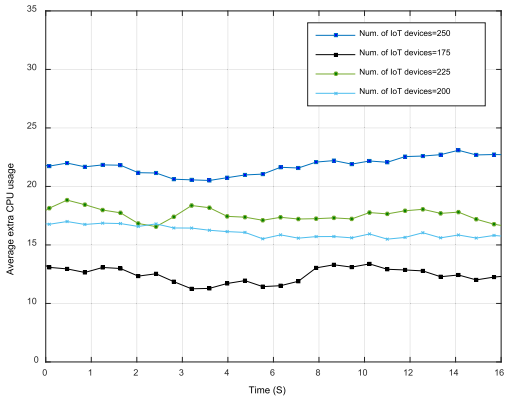

FIGURE 5. Overhead.

The brief spike before execution corresponds to the code reconstruction, while the brief spike after execution corresponds to the serialization process, for which a small memory surge can also be observed. We have shown how high the overhead is for IoT devices.

As Fig. 3 reveals, our solution incurs at most 10-18% overhead on IoT devices. Therefore, we can use our solution on IoT devices that can handle this amount of overhead.

In the future, we plan to evaluate the proposed method from different aspects, such as the number of successful attackers trying to find sensitive data. Also, we plan to evaluate our solution when the distribution time period varies.

VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a solution to increase the amount of privacy of IoT devices in a smart city. To this aim, we proposed a Software Defined Networking-inspired paradigm called DPSmartCity. It comprises two parts, the equipment of an IoT-based smart city with the SDN paradigm and a mounted privacy-preserving method on top of it, which uses different Differential Privacy distributions over time. In our solution, we apply the Differential Privacy method, which frequently uses either the Laplace distribution or the exponential distribution. The Differential Privacy distribution is changed every minute by the devices. As results show, compared to current studies, we have achieved a more effective environment that protects sensitive information from unwanted disclosure. By leveraging our solution, adversaries cannot discover sensitive data as easily as with a traditional static privacy-preserving method.

Experiments showed that the DPSmartCity method incurs at most 10–18% overhead on IoT devices. Therefore, our solution can be used for IoT devices that can handle this amount of overhead. We plan to evaluate our solution based on more evaluation metrics, such as accuracy, in future.

REFERENCES

[1] M. Gheisari et al., "NSSSD: A new semantic hierarchical storage for sensor data," in *Proc. IEEE 20th Int. Conf. Comput. Supported Cooperative Work Des.*, 2016, pp. 174–179.

[2] A. Javadpour, A. M. H. Abadi, S. Rezaei, M. Zomorodian, and A. S. Rostami, "Improving load balancing for data-duplication in big data cloud computing networks," *Cluster Comput.*, no. 4, pp. 2613–2631, 2021.

[3] A. Jalili., "A new SDN-based framework for wireless local area networks," *Int. J. Nonlinear Anal. Appl.*, vol. 10, no. 1, pp. 177–183, 2019.

[4] A. Javadpour, "Providing a way to create balance between reliability and delays in SDN networks by using the appropriate placement of controllers," *Wireless Pers. Commun.*, vol. 110, pp. 1057–1071, 2020.

[5] A. Javadpour, "Improving resources management in network virtualization by utilizing a software-based network," *Wireless Pers. Commun.*, vol. 106, no. 2, pp. 505–519, 2019.

[6] F. Ja'fari, S. Mostafavi, K. Mizanian, and E. Jafari, "An intelligent botnet blocking approach in software defined networks using honeypots," *J. Ambient Intell. Hum. Comput.*, vol. 12, pp. 2993–3016, 2021.

[7] F. Knirsch, D. Engel, C. Neureiter, M. Frincu, and V. Prasanna, "Privacy assessment of data flow graphs for an advanced recommender system in the smart grid," in *Proc. Int. Conf. Inf. Syst. Secur. Privacy*, 2015, pp. 89–106.

[8] A. Javadpour, G. Wang, and S. Rezaei, "Resource management in a peer to peer cloud network for IoT," *Wireless Pers. Commun.*, vol. 115, pp. 2471–2488, 2020.

[9] M. Gheisari, G. Wang, M. Z. A. Bhuiyan, and W. Zhang, "MAPP: A modular arithmetic algorithm for privacy preserving in IoT," in *Proc. IEEE Int. Symp. Parallel Distrib. Process. Appl. IEEE Int. Conf. Ubiquitous Comput. Commun.*, 2017, pp. 897–903.

[10] F. Liu and T. Li, "A clustering-anonymity privacy-preserving method for wearable IoT devices," *Secur. Commun. Netw.*, pp. 1–8, 2018.

[11] M. Gheisari, G. Wang, and S. Chen, "An edge computing-enhanced Internet of Things framework for privacy-preserving in smart city," *Comput. Elect. Eng.*, vol. 81, 2020, Art no. 106504.

[12] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[13] A. J. Moshayedi, A. S. Roy, A. Taravet, L. Liao, J. Wu, and M. Gheisari, "A secure traffic police remote sensing approach via a deep learning-based low-altitude vehicle speed detector through UAVs in smart cites: Algorithm, implementation and evaluation," *Future Transp.*, vol. 3, pp. 189–209, 2023, doi: 10.3390/futuretransp3010012.

[14] M. Gheisari, G. Wang, S. Chen, and A. Seyfollahi, "A method for privacy-preserving in IoT-SDN integration environment," in *Proc. IEEE Int. Conf. Parallel Distrib. Process. Appl., Ubiquitous Comput. Commun., Big Data Cloud Comput., Social Comput. Netw., Sustain. Comput. Commun.*, 2018, pp. 895–902.

[15] T. Peng, Q. Liu, and G. Wang, "A multilevel access control scheme for data security in transparent computing," *Comput. Sci. Eng.*, vol. 19, no. 1, pp. 46–53, Jan/Feb. 2017.

[16] M. Gheisari, G. Wang, W. Z. Khan, and C. F. Campusano, "A context-aware privacy-preserving method for IoT-based smart city using software defined networking," *Comput. Secur.*, vol. 87, 2019, Art no. 101470.

[17] A. Jalili and M. Keshtgari, "A new reliable controller placement model for software-defined WANs," *J. AI Data Mining*, vol. 8, no. 2, pp. 269–277, 2020.

[18] A. Javadpour and G. Wang, "cTMvSDN: Improving resource management using combination of Markov-process and TDMA in software-defined networking," *J. Supercomput.*, pp. 1–23, 2022.

[19] M. A. Jahangir et al., "Automation attendance systems approaches: A practical review. BOHR international journal of Internet of Things," *Artif. Intell. Mach. Learn.*, vol. 1, no. 1, pp. 23–31, 2021, doi: 10.54646/bijiam.005.
[20] M. Safaei Yaraziz et al., " Recent trends towards privacy-preservation in Internet of Things, its challenges and future directions," *IET Circuits Devices Syst.*, pp. 1–9, 2022, doi: 10.1049/cds2.12138.
[21] M. AJ et al., "Simulation and validation of optimized PID controller in AGV (automated guided vehicles) model using PSO and BAS algorithms," *Comput. Intell. Neurosci.*, vol. 2022, 2022, Art. no. 7799654, doi: 10.1155/2022/7799654.
[22] Y. Liu et al., "CFDMA: A novel click fraud detection method in mobile advertising," in *Proc. 4th Int. Conf. Data Intell. Secur.*, 2022, pp. 394–401.
[23] N. K. Kamila et al., "A near-optimal & load balanced resilient system design for high-performance computing platform," *Cluster Comput.*, pp. 1–6, 2023, doi: 10.1007/s10586-022-03913-8.
[24] M. Mangla et al., "A proposed framework for autonomic resource management in cloud computing environment," in *Autonomic Computing in Cloud Resource Management in Industry 4.0*. Berlin, Germany: Springer, 2021, pp. 177–193.

MEHDI GHEISARI received the B.S. degree in computer engineering from Shiraz University, Shiraz, Iran, and the M.Sc. degree in computer engineering from Science and Research University, Tehran, Iran. He is currently working toward the Ph.D. degree with the School of Computer Science and Educational Software, SUSTECH, Shenzhen, China. He has taught in variety of Universities as a Professor of courses like data base and operating system. Since 2007, he has been with Karaj University, Karaj, Iran, ShamsiPour College, Bahonar College, Damavand branch, Parand Branch, Islamic Azad University, Tehran, Iran. He has authored or coauthored 13 research articles in journals and 29 conference papers, one book and two patents contributed as author/co-author. His research interests include wireless sensor networks (monitoring, routing, event detection), semantic web and related technologies (RDF, ontologies), and programming (Net). He is a Member of Geo-Information and Communication Technology Society, Young Researchers Club of IAU, and an Associative Member of the Universal Association of computer of Computer & Electronics Engineers. He is alos an Associate Editor and Reviewer of ISI journal, such as the *Indian Journal of Science and Technology*, Reviewer of the *International Journal of Wireless Information Networks*, WSEAS journals in the field of semantic web and sensor networks, *International Journal of Computer and Information Technology*, and an Expert Reviewer and the Guest Editor of the *Indian Journal of Innovations and Developments*.

EHSAN SHOJAEIAN received the B.S. degree in computer engineering from Razi University, Kermanshah, Iran, and the M.S. degree in computer engineering from Science and Research University, Tehran, Iran. He is currently a Research Scholar with the Department of Computer Engineering, SRBIAU, Tehran, Iran.

AMIR JAVADPOUR received the M.Sc. degree in medical information technology engineering from the University of Tehran, Tehran, Iran, in 2014, and the Ph.D. degree in computer science (mathematics/cybersecurity) from Guangzhou University, Guangzhou, China, in 2020. He has authored or coauthored papers with his colleagues in highly ranked journals and several ranked conferences on several topics, including *Cloud Computing*, *Software-Defined Networking*, *Big Data*, *Intrusion Detection Systems* (IDS), and *Internet of Things*, *Moving Target Defence*, *Machine Learning*, and *Optimization Algorithms*. He reviewed papers for several reputable venues, such as IEEE TRANSACTIONS ON CLOUD COMPUTING, IEEE TRANSACTIONS ON NETWORK SCIENCE AND ENGINEERING, *ACM Transactions on Internet Technology*, *Journal of Supercomputing*, several journals of Springer and Elsevier. He is also the Technical Program Committee Member of various conferences.

AHMAD JALILI received the Ph.D. degree in information technology from the Shiraz University of technology, Shiraz, Iran. Ahmad is an Assistant Professor with the Department of Computer Engineering at Gonbad Kavous University, Golestan, Iran.

HAMID ESMAEILI-NAJAFABADI, biography not available at the time of publication.

BAHRAM SADEGHI BIGHAM received the M.Sc. degree in 2000 and the Ph.D. degree from the AmirKabir University of Technology (Tehran Polytechnic), Tehran, Iran. He is currently an Assistant Professor with the Department of Computer Science and Information Technology, Institute for Advanced Studies in Basic Sciences, where he directs the RoboCG lab. He has authored or coauthored five books, one book chapter 14 articles in journals, 12 papers in conferences. His research interests include robot motion planning, computational geometry, algorithms and graphs, computer vision, and AI. His research interest related to Computational Geometry Pages, The Open Motion Planning Library, Motion Strategy Library. He was a Postdoctoral Fellow with the School of Computer Science, University of Cardiff, Cardiff, U.K. He is a Member of following scientific societies Schools on Computational Geometry, Computer Science Conference on Computer and Information Technology, Conference on Computer Science New Topics (Alzahra University International Conference on Computer, Information Technology and Digital Media (CITaDiM), and Scientific Manager. He is also Guest Reviewer of number of national and international journals.

ALISA A. VOROBEVA is currently an Assistant Professor with the National Research University of Information Technologies, Mechanics and Optics, St Petersburg, Russia. Her research interests include cyber security, forensic linguistics, natural language processing, opinion mining, and web user identification.

YANG LIU received the bachelor's degree in computer science from the Ocean University, Qingdao, China, and the M.Sc. degree in software engineering from Peking University, Beijing, China. He is currently an Assistant Professor with the Department of Computer Science and Technology, Harbin Institute of Technology, Shenzhen, China. His research interests include security and privacy problems and, in particular, privacy issues on mobile devices.

MOHAMMAD REZAEI, biography not available at the time of publication.