Available online at www.sciencedirect.com
ScienceDirect
journal homepage: www.elsevier.com/locate/cose
Computers & Security

A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking

Mehdi Gheisari[a], *Guojun Wang*[a,*], *Wazir Zada Khan*[b], *Christian Fernández-Campusano*[c]

[a] *School of Computer Science, Guangzhou University, Guangzhou 510006 China*
[b] *Farasan Networking Research Laboratory, Faculty of CS & IS, Jazan University, Jazan 45142, Saudi Arabia*
[c] *University of the Basque Country UPV/EHU, Donostia-San Sebastián, 20018, Spain*

ARTICLE INFO

Article history:
Received 22 November 2018
Revised 24 January 2019
Accepted 14 February 2019
Available online xxx

Keywords:
SDN
IoT
Privacy
Context-aware
Dynamic
Internet of Things
Penetration rate
Software Defined Networking
Smart city
VPN

ABSTRACT

Smart City is an application of the Internet of Things (IoT) with the aim of managing cities without human intervention. Each IoT device that is producing data may sense a sensitive one that should not be disclosed unintentionally. Due to the existence of a large number of devices in the near future, the possibility of information leakage, privacy breach, is increasing. To prevent this, each device applies a privacy-preserving method. We discover that all of the existing solutions have three major drawbacks: (1) applying one static privacy-preserving method for the entire system, (2) sending whole data at once, and (3) not context-aware. These cause unacceptable privacy-preserving degree. To address them, in this paper, at first, we equip IoT-based smart city with Software Defined Networking paradigm (SDN). Then, we mount an efficient privacy-preserving method on top of it that manages flowing data packets of split IoT device' data. We have done extensive simulation through MININET-WIFI to show the effectiveness of our approach. Evaluation results show that our method can be widely applied to the smart city application with a superior performance regarding accuracy, overhead, and penetration rate compared to existing privacy-preserving solutions.

1. Introduction

IoT is connecting all the things around the world through the Internet. The things refer to the objects that are built-in/equipped with a unique Identifier such as IP (Liu et al., 2017a). These objects should act automatically and without any human intervention. Based on the predictions, the number of devices that perform actions automatically will reach billions by 2020 (Gheisari et al., 2019; M et al., 2017; Yari et al., 2017). This large number of devices brings excellent capability, providing quality services through produced data, if we propose schemes that can manage them well. Otherwise, it makes a barrier to use it in widespread mode.

On the other hand, current cities managements are suffering from critical issues such as public transportation management, energy management of citizens, waste management and so on. These issues become more critical when, based on the predictions, the world population will hugely increase by 2050 (Sethuraman et al., 2019;

[*] Corresponding author.
E-mail addresses: mehdi.gheisari61@gmail.com (M. Gheisari), csgjwang@gzhu.edu.cn (G. Wang).

https://doi.org/10.1016/j.cose.2019.02.006
0167-4048/© 2019 Published by Elsevier Ltd.

Fig. 1 – Smart city environment.

United Nations and Affairs, 2002). IoT paves the way to be facilitated with traditional cities in order to manage cities automatically and to solve their issues, smart cities. One technology that paves the path for automatic management of cities efficiently is equipping the traditional cities with IoT called smart city. If the management is done well, it will have a great impact on the quality of life (Alzubi et al., 2018a; Alzubi et al., 2018b; M et al., 2017; Rezaeiye et al., 2017).

Although smart city brings excellent opportunity, due to the existence of large number of devices that are acting without human intervention, it increases the possibility of information leakage because of devices may produce sensitive data (Gheisari et al., 2017). Sensitive data refers to the data that if it reveals, the possibility of harming system will increase. So, we should provide solutions to be applied in order to prevent disclosure of sensitive data, privacy-preserving (Liu et al., 2017a; Peng and Wang, 2017; Yu et al., 2015; Zhang et al., 2018).

Recently, privacy-preserving of IoT devices' data has received a great deal of attention in the security community (Gheisari et al., 2018; Liu et al., 2017b; Sharma et al., 2017; Zhang et al., 2017a; Zhang et al., 2017b). Through observation, we discovered that all proposed solutions are focusing on applying static privacy-preserving methods for the entire system. In other words, the entire system applies one/more static privacy-preserving methods. In addition, IoT devices send whole data at once. These pose huge vulnerability to the system and reducing privacy-preserving level. In the optimistic case, if the method is very efficient, one penetration -stems from unwanted activities such as attackers- is enough to make harm to the system due to the possible collaboration of malicious activities with each other. If one malicious activity finds how to penetrate the system, it can notify others. So, the rests can penetrate easier (M et al., 2015).

The main concept is illustrated in Fig. 1. It depicts a system overview of the smart city environment where IoT devices send their data directly to the Cloud Computing environment for further analysis (Zhang et al., 2018).

Moreover, in traditional networking paradigms, switches are fully-built (Alzubi et al., 2018b). It means Control plane and Data plane of each switch are integrated. Data plane has the duty of forwarding data packets. And, Control plane is the part of the network that carries signaling traffic and in charge of routing. Recently, a networking paradigm emerged called Software Defined Networking (SDN) that the Control plane and the Data plane is separated (Abawajy et al., 2016; M.Gheisari and M.Esnaashari, 2019). Instead of having fully-built switches, switches are dumb ones, often, OpenFlow switches (Antikainen et al., 2014). These dumb switches are plain hardware that only has the duty of forwarding data packets. And, the Control plane manages them. This management is done by one or more SDN controllers. In short and straightforward, with the help of the SDN paradigm, we are able to manage data packets in the networks.

In this paper, we present an efficient method for privacy-preserving in a smart city that is facilitated with the SDN paradigm. In detail, at first, we equip IoT-based smart city with the SDN paradigm. Then, we propose a method on top of it to preserve the privacy of all kinds of IoT devices with different degrees of privacy-preserving levels. The privacy is achieved through managing data packets that are flowing in the network.

In detail, based on the amount of the data sensitivity, context-awareness, the SDN controller makes a decision for each IoT device. Being context-aware is important particularly for dynamic environments due to the fact that decisions should be made based on the context. If the data is not high sensitive, the device should split its data and sends each part through the chosen routes. On the contrary, if it is high sensitive, the IoT device will split its data and will send the first part from a secure route and the second part from a created Virtual Private Network (VPN) by the SDN controller (Liu et al., 2017b). In the end, the SDN controller will update the amount of the devices data sensitivity. It is notable to mention that the amount of sensitivity can be changed over time. In this manner, unwanted activities should be very brilliant in order to find flowing sensitive data.

The major contributions of this paper are three-fold:

- We facilitate IoT-based smart city environment with SDN paradigm in order to have a more flexible and agile network.
- We propose a privacy-preserving method on top of the equipped city. This is achieved through the fact that the SDN controller manages the data packets of all IoT devices and it splits their data based on the context.
- Finally, we validate our method in extensive simulations. We have found that it achieves a superior performance in terms of accuracy, the amount of overhead, and penetration rate compared to the existing privacy-preserving schemes.

This paper is organized as follows. Section 2 reviews related work. Section 3 formulates our problem and focuses on the IoT-based smart city environment that is equipped with the SDN paradigm, then, focuses on our privacy-preserving method on top of the equipped environment. Evaluation through simulation and mathematical proof is conducted in Section 4. Moreover, Section 5 discusses achievements and drawbacks of our solution. Finally, Section 6 concludes this paper and propose future work.

2. Related work

In this section, we focus on the existing solutions that are trying to solve privacy-preserving issue in the IoT-based smart city environment with the leveraging of the SDN paradigm. To the best of authors' knowledge, and based on (Kalkan and Zeadally, 2018) several studies have been done to secure IoT with leveraging SDN, but regretfully, a very few researches have been performed for privacy-preserving in IoT-based smart city using SDN.

Authors in Chakrabarty et al. (2015) proposed a secure networking mechanism for IoT-SDN environment. They mitigated data gathering through encrypting not only the payload, but also the header of source and destination IP addresses. They proposed a routing protocol with the utilization of an SDN controller. Their secure routing brings privacy due to only intended recipient gets the data destined for it (Wang et al., 2011). They considered asynchronous node “sleep” and “wake” cycles. Beyond the fact that it brings privacy-preserving in IoT-SDN environment, it saves energy consumption of the network too. However, one of the major drawbacks of it is that it only provides privacy-preserving through applying one static encryption method. So, the privacy-preserving level of it is not acceptable. One penetration is enough to break the entire solution.

We in Gheisari et al. (2018) proposed a solution for privacy-preserving in IoT-SDN environment. We preserved the privacy through providing a dynamic environment for IoT devices from privacy-preserving point of view. We achieved privacy by dividing IoT devices into two categories and each category applies its own special privacy-preserving method. Although it provides in acceptable privacy-preserving level, it has one drawback that is it encrypts whole data if it is highly sensitive. This leads to high-computational cost.

In Mehdi Gheisari (11-13 Dec. 2018, Melbourne, Australia), we took one step further and proposed a method that leveraged several privacy-preserving and security techniques in order to preserve the privacy of generated data. We provided a highly dynamic environment so that each device was able to apply one out of six possible methods, four encryption methods or an aggregation method or a VPN method. If the aggregation method is selected for applying as the privacy-preserving method, the device aggregates the last 5 s of its data. Although the solution has several benefits such as low penetration rate and preserves the privacy of sensitive data at an acceptable level, its computational cost is high. In addition, the SDN decision is not context-aware. It means that the controller does not make decision based on the context.

In order to alleviate the possibility of finding sensitive data while it is tolerable to most IoT devices, in this paper, we propose a privacy-preserving solution in IoT-based smart city environment utilizing SDN paradigm. The SDN controller makes decisions about how IoT devices should behave with their data based on the sensitivity level of the data, context-awareness. The necessity of being context-aware for a solution highlights more when the environment is highly-dynamic. Moreover, privacy-preserving is achieved through splitting IoT device data. And, the SDN controller manages the flowing split data. If the data is non-sensitive, it assigns two common routes then, the IoT device sends its split data through the routes. And, if the data is highly sensitive, the IoT device splits its data, and the controller asks the device to send its first part through a secure founded route and the second part from a created VPN.

3. Proposed framework for IoT-based smart city

In this section, we focus on our solution that preserves the privacy of IoT-based smart city environment that is equipped with SDN paradigm efficiently. Our solution consists of two steps. (1) equipping the environment with SDN technology, and (2) a method on top of the enhanced environment to preserve the privacy.

3.1. *Equipped IoT-based smart city with SDN paradigm*

In this section, we equip an IoT-based smart city with the SDN paradigm to able to manage data packets centrally and in a flexible manner. Thus, we achieve a flexible and an agile environment.

Fig. 2 illustrates the ecology, our scenario network model.

In our scenario, there are six devices: a smartwatch, a smart building, a smartphone, a laptop, a waste can, and one autonomous vehicle. These devices are connected to an SDN controller through two OpenFlow switches. The SDN controller has a mutual relationship with the Cloud Computing environment. For example, the smart building collaborates with the Cloud through one of the OpenFlow switches and the SDN controller. These two switches are controlled by the SDN controller. And, in turn, the SDN controller sends their data to the Cloud environment for further analysis. We assume that all of the devices as mentioned above are producing sensitive data except “waste can” and smartphone device that are not producing highly sensitive data. Thus, in this paper, we do not allow the unwanted disclosure of all produced data except those stem from waste can and smartphone. The SDN controller based on the amount of sensitivity level of IoT devices, highly sensitive or not, decides how each IoT device should behave with its data.

3.2. *Mounted privacy-preserving method on the equipped environment*

Privacy refers to the states or conditions of being free from being observed and disturbed by others; unwanted parties cannot find sensitive data (Chen et al., 0000; Kalkan and Zeadally, 2018; Wang et al., 2017; Zhang et al., 2018; Zhang et al., 2019). To this aim, we propose a privacy-preserving method that is mounted on the enhanced IoT-based smart city with the SDN paradigm based on secure routing. We gain privacy due to sensitive data does not be disclosed unintentionally and it is very

Please cite this article as: Mehdi Gheisari, Guojun Wang and Wazir Zada Khan et al., A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking, Computers & Security, https://doi.org/10.1016/j.cose.2019.02.006

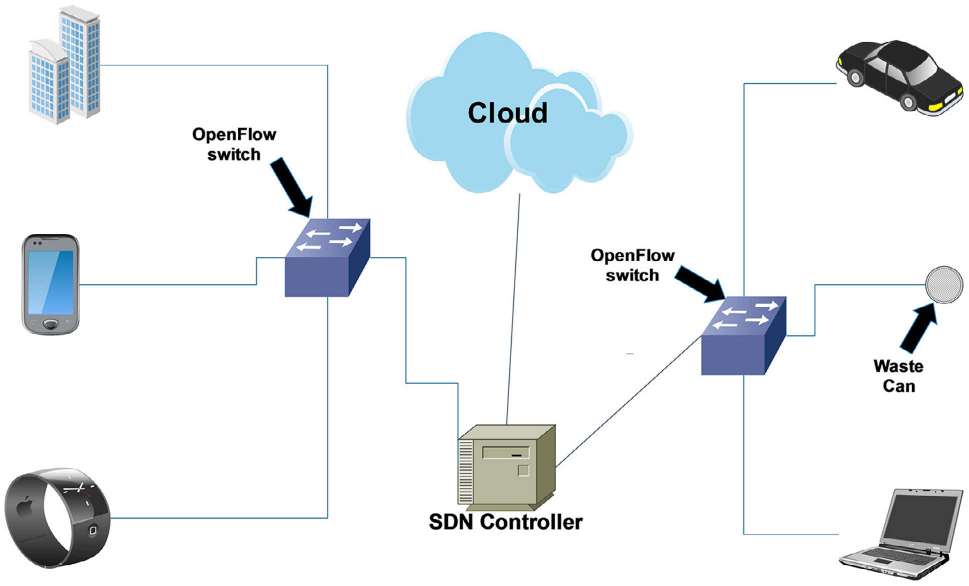

Fig. 2 – Equipped smart city.

difficult for unwanted parties to find original data. In our scenario, OpenFlow switches are dumb and the data plane and control plane is separated, the SDN controller controls the data flow of the network. We leverage this capability in order to provide an environment that it is efficient from the privacy-preserving dimension (Gheisari and Bagheri, 2011).

In our scenario, each device splits its data into two parts based on the received command from the SDN. In the received command, the SDN declares two information: (1) in which way the IoT device should split its data, and (2) how the IoT device should behave with each part. The SDN controller makes decisions based on two predetermined information that are stored in two databases: (1) information about the sensitivity level of IoT devices' data, and (2) the information about credits of routes, how much they are secure.

Fig. 3 illustrates the flowchart of our proposed method, a privacy-preserving method in the IoT-based smart city using SDN paradigm, step by step.

In detail, each device asks from the SDN controller, what it should do with its data while it sends its ID to the SDN controller. Then, based on the device ID, if the device produces highly sensitive data, the SDN controller asks the IoT device to split its data into 70% and 30%. We assume that the devices' experts, already in a database, put possible generating data along with the information that whether the generated data is sensitive or not (ARIF et al., 2018; Kia et al., 2018; Wang et al., 2018). Moreover, the amount of split is assumed. The best amount of split is needed to be investigated, one of future work. Next, the controller determines the most secure route in the network based on a prefilled data base and notifies the device. Then, the IoT device will send its first part from the route. Next, the SDN controller will create a VPN from the device to itself and informs the device (Peng et al., 2017). In brief and straightforward, VPN is a technology that creates a safe and encrypted connection over less secure networks, such as the internet. It does not allow unwanted access to sensitive data from outside point of view. And, the IoT device will send its remaining, 30%, data, through the created VPN to the SDN controller. Next, the SDN controller merges the received data. Then, it sends integrated data to the Cloud for further analysis.

On the other hand, if the sensitivity amount of the IoT device data is low, the SDN controller asks the device to split its data into two halves. The best amount of the split is needed to be investigated more. Then, the controller specifies two different routes based on the prefilled database and informs the device. Next, the device sends each part from one determined route. Finally, the SDN controller integrates the received partial data and will send it to the Cloud. This process is iterative.

From an abstract point of view, the SDN controller already knows that each IoT device in the smart city is (1) high sensitive, the generated data is very critical and should not be disclosed unintentionally, or (2) low sensitive, their data is not very critical to be disclosed. In addition, it has information about the secure routes in the network. Then, based on the device ID, if the device is producing highly sensitive data, the device splits its data into two parts, 70%, and 30%. Then, the controller finds the most secure route. Next, the device sends the first part through the secure route. And, the second part will be sent through a created VPN by the SDN controller. In reverse, if the device data is not very sensitive, the SDN controller specifies two routes and informs the device. Next, the device sends each part of its data through a determined route. Whether the data is highly sensitive or not, the controller integrates received data and sends it to the Cloud.

4. Performance evaluation

In this section, we evaluate our solution from different aspects in order to show its superior performance.

We assumed that, in our scenario, unwanted malicious parties are trying to find the original generated data. In addition, the SDN controller is completely trustful and does not

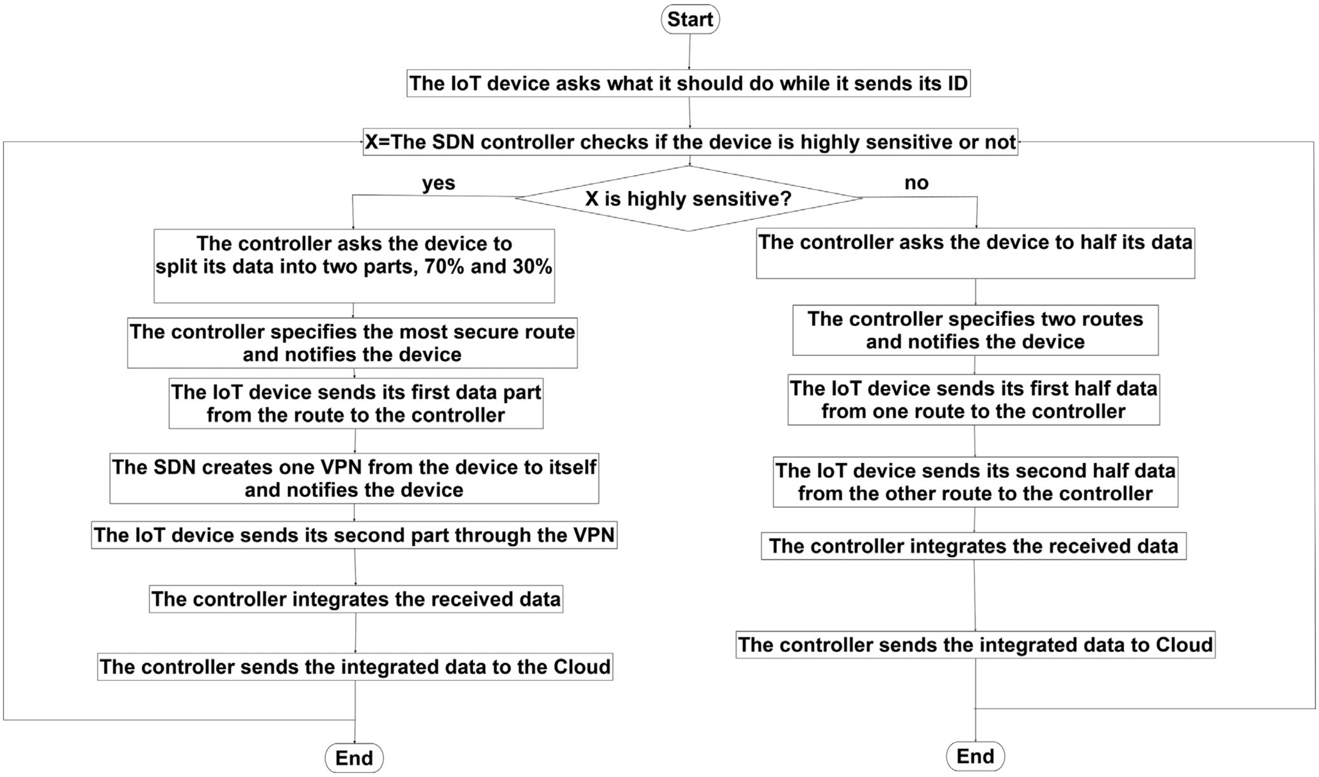
Start
The IoT device asks what it should do while it sends its ID
X=The SDN controller checks if the device is highly sensitive or not
yes
X is highly sensitive?
no
The controller asks the device to split its data into two parts, 70% and 30%
The controller specifies the most secure route and notifies the device
The IoT device sends its first data part from the route to the controller
The SDN creates one VPN from the device to itself and notifies the device
The IoT device sends its second part through the VPN
The controller integrates the received data
The controller sends the integrated data to the Cloud
End
The controller asks the device to half its data
The controller specifies two routes and notifies the device
The IoT device sends its first half data from one route to the controller
The IoT device sends its second half data from the other route to the controller
The controller integrates the received data
The controller sends the integrated data to Cloud
End

Fig. 3 – Proposed method step by step.

perform any malicious activities. We simulate our scenario using MININET-WIFI software (Al-Badarneh et al., 2017). Algorithm 1 shows our privacy-preserving solution in the IoT-based smart city equipped with SDN paradigm. “I” refers to the device ID. “S(i)” refers to the result of a sub procedure that returns the value if the IoT device is sensitive or not. “R(i)” refers to an appropriate selected route that is from the device to the SDN controller. “R2(i)” refers to other selected appropriate route that is from the device to the SDN controller. “SP(i,a,b)” is a procedure that splits device data of I into two parts, “a” percent and “b” percent. “VPN(i)” is another procedure that creates a VPN from the device to the controller.

Algorithm 1

```
procedure PRIVACY-PRESERVING SOLUTION
Input: Two information about the sensitivity of the devices and secure routes
Output: Safe environment
    for $i = 2$ to $n$ do
        if S(i) = Yes then
            X,Y=SP(i,70,30)
            Sending X through R(i)
            Sending Y through VPN(i)
        if S(i) = No then
            X,Y=SP(i,50,50)
            Sending X through R(i)
            Sending Y through R2(i)
```

There are five evaluation metrics for evaluation of a privacy-preserving method that are (Gheisari, 2012):

1. Completeness and Consistency: Calculating the amount of unused and non-important data compared to the original data set.
2. Scalability: Calculating the amount of performance increase when the number of IoT devices is increased.
3. Penetration rate: Calculating the number of successful malicious activities that can find the original data.
4. Overload: Calculating the amount of computational cost and overload imposed on the system.
5. Accuracy: Calculating the amount of information loss.

From the authors’ point of view, among the five dimensions as mentioned earlier, the last three parameters are more critical to be calculated and evaluated. So, for evaluation of our method, we calculate the amount of the accuracy, penetration rate, and overload to the system. We simulate our scenario that is depicted in Fig. 2.

4.1. *Accuracy*

Accuracy shows how much the data reflects the truth. It is one of the components of data quality. It refers to whether the processed data values, after performing the privacy-preserving solution, are in the correct forms or not. In short, we calculate how much information is lost after applying the privacy-preserving solution (Jafari et al., 2016). After evaluation, we have found the amount of information loss is zero due to we

Please cite this article as: Mehdi Gheisari, Guojun Wang and Wazir Zada Khan et al., A context-aware privacy-preserving method for IoT-based smart city using Software Defined Networking, Computers & Security, https://doi.org/10.1016/j.cose.2019.02.006

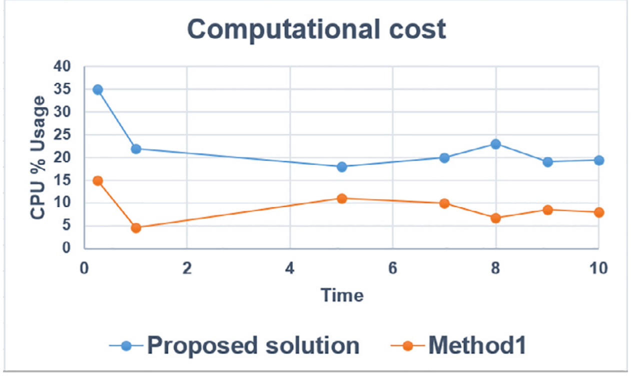

Fig. 4 – Computational cost of the proposed method during time.

address all of the data packets and our solution does not ignore any sensitive packet. The privacy of data is kept without losing even one byte of sensitive data.

4.2. *Overload*

For evaluating our solution to find how much overload it imposes on the system, two evaluation metrics are used: Computational complexity and Computational cost.

4.2.1. *Computational complexity*

In this part, we calculate the amount of the overload of our solution imposes on the system theoretically. Computational complexity refers to the Order of growth of an algorithm that is a way of predicting how will be the execution time of a program and the occupied memory when the input size increases. In simple, it is used to describe the execution time required or the space used, in memory or on disk, by an algorithm. The most famous symbol is the Big-O notation (Papadimitriou, 2003). Big-O describes the worst-case scenario explicitly. After calculation, we have found the Big-O of the algorithm is $O(3 \times n)$. N is the number of devices. $O(3 \times n)$ illustrates that for each device utmost three significant extra processes are required. It means that if the number of devices increases, the stronger SDN server is needed.

4.2.2. *Computational cost*

We should prove that the proposed method is applicable to IoT devices and they can afford the extra computational cost due to most of the IoT devices are resource-constraint. We calculate how much computational cost is imposed on the IoT-based smart city by our solution through simulation. In the traditional systems, each device sends its data to the Cloud directly (Liu et al., 2017c; Wang et al., 2013). But in our solution, as mentioned above, with the usage of the SDN controller, each device should process more steps to send its data to the Cloud while preserving the privacy.

Fig. 4 illustrates the amount of computational cost of our solution that poses to the environment within 10 s and we compare it with the computational cost of the introduced method in Mehdi Gheisari (11-13 Dec. 2018, Melbourne, Australia) called Method1. In Method1, IoT devices are categorized into three classes. And, each category uses a different method to hide the generated sensitive data that can be encryption, aggregation or sending its sensitive data through a created VPN.

As far as Fig. 4 shows, in average the amount of computational cost overhead is around 35%, except the start time that all devices are rushing to the SDN controller to find what they should do.

4.3. *Penetration rate*

To show how much our privacy-preserving solution is effective, we need to calculate the penetration rate too. Penetration rate refers to the number of successful unwanted activities that are able to find sensitive data and harm the system (Rezaeiye et al., 2017).

There are mainly two types of malicious activities that are trying to find original data (Chen et al., 2014; Nazir et al., 2015): (1) Content, and (2) Context one. In the content type, the malicious activity is trying to find the generated data. However, in context one the main focus is not the sensed data; the main focus is finding related information about the data such as the time of sensing. Here, we assume that two content activities are trying to penetrate the system. One of them is a simple outsider malicious activity called simple attack, without any intelligence about the environment. It does not have any background information such as the IoT devices' data are divided. So, if it finds the data, it has achieved faulty data. It only sniffs the network. And, the second malicious activity called linked data attack, has a small amount of background information about the system. Information about the fact that all passing data are not whole data, and if it wants to find the whole sensitive data, it should attack two parts in order to achieve the data of one device, for non-highly sensitive devices two different routes and for highly sensitive devices: one secure route and one VPN. We assume that the SDN controller is trustful, and it does not include any malicious activities.

we calculated the amount of the time two malicious activities needed to penetrate the system. Among the two simulated, both were unsuccessful in finding the sensitive data. The first one who did not have any background information was utterly unsuccessful in locating the whole sensitive data. It found only the first part of the sensitive data after 0.4 s that was very late. And, the second one that knew it should attack two sections of the network to find a data and which parts of the network tried to attack the created VPN from the device to the SDN controller, but the penetration was not successful. Its attempt took 0.7 s. On the other hand, after 6.1 s the sensitivity degree of the device had changed, and the SDN controller had selected another behavior for the device to apply, two different routes.

Fig. 5 shows the penetration time that is required by malicious activities to penetrate the system in a schematic form.

5. Discussion

In this section, we discuss the performance of our solution.

Based on the results, we have found that our solution does not have any sensitive information loss. It means that we are

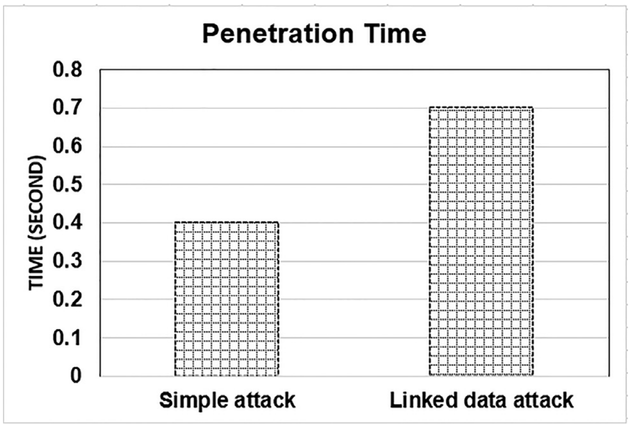

Fig. 5 – Spent time to penetrate the system.

sure that no information misses, accuracy. Thus, we can rely on the solution from this dimension.

In addition, we evaluated our solution from the amount of the overload point of view. Theoretically, we showed that the computational complexity of our solution is O(3 × n). It shows that, in the worst case, our solution with the increase in the number of devices suffers three more significant tasks. Moreover, from the computational cost aspect, we have found that our solution poses 35%. With the current advancement in technology, IoT devices are less resource-constraint so many IoT devices can afford this amount of the overhead. Although the amount of the overhead is affordable, it is better to do not use the solution for resource-constraint devices.

Moreover, we calculated the penetration rate of our solution, how much it is robust in order to malicious activities such as attackers cannot find the original sensitive data. Among the two attackers, both were unsuccessful. This shows that our solution is also robust against stealing data and disclosing data to unwanted parties. Thus, it can be considered as the complementary of security guards. In simple, if a malicious actvity wants to find sensitive data and the security mechanism of the system is unable to make a barrier, our solution will hinder the it.

Our solution can be generalized to all types of IoT devices. Thus, it can be used widely in IoT applications such as smart city.

6. Conclusion

In this paper, we proposed a privacy-preserving solution for an equipped IoT-based environment using the SDN paradigm. The SDN controller, based on the amount of sensitivity level of the IoT devices' data and credits of the routes, decides how IoT devices should behave with their data. We showed that the privacy is preserved through splitting sensitive data and sending split parts through a secure route and a VPN. We showed our proposed solution is accurate and no sensitive information is lost. Moreover, we demonstrated that our solution imposes at most 35% overhead to the system. Although 35% is acceptable for current advanced IoT devices, it would be better to use it for not resource-constraint devices. In addition, we proved that our solution supports the security mechanisms and reimburses their drawbacks. In short and straightforward, if the system is penetrated due to the drawbacks of security schemes, our solution can hinder malicious activities too. One future work is involving more metrics so that the SDN controller can make high-level decisions.

Conflicts of interest

No potential conflict of interest was reported by the authors.

Ethical approval: This article does not contain any studies with human participants performed by any of the authors.

Acknowledgments

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

Supplementary material

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.cose.2019.02.006.

REFERENCES

Abawajy JH, Wang G, Yang LT, Javadi B. Trust, security and privacy in emerging distributed systems. Future Gen Comput Syst 2016;55:224–6.

Al-Badarneh J, Jararweh Y, Al-Ayyoub M, Al-Smadi M, Fontes R. Software defined storage for cooperative mobile edge computing systems. In: Proceedings of the fourth international conference on software defined systems (SDS), 2017. IEEE; 2017. p. 174–9.

Alzubi Jafar A and Yaghoubi A, Gheisari M, Qin Y. Improve heteroscedastic discriminant analysis by using CBP algorithm. In: Proceedings of the algorithms and architectures for parallel processing. Cham: Springer International Publishing; 2018a. p. 130–44.

Alzubi JA, Shahabi AS, Fernndez-Campusano C, Gheisari M, Qin Y. A new algorithm for cluster leader selection in wireless sensor networks. Proceedings of the ICAC 2018, UK. IEEE, 2018b.

Antikainen M, Aura T, Särelä M. Spook in your network: attacking an SDN with a compromised openflow switch. In: Proceedings of the Nordic conference on secure IT systems. Springer; 2014. p. 229–44.

ARIF M, WANG G, BALAS VE. Secure vanets: trusted communication scheme between vehicles and infrastructure based on fog computing. Stud Inform Control 2018;27(2):235–46.

Chakrabarty S, Engels DW, Thathapudi S. Black SDN for the internet of things. In: Proceedings of the 2015 IEEE 12th international conference on mobile ad hoc and sensor systems; 2015. p. 190–8. doi:10.1109/MASS.2015.100.

Chen S., Wang G., Yan G., Xie D.. Multi-dimensional fuzzy trust evaluation for mobile social networks based on dynamic community structures. Concurr Comput: Pract Exp; 29(7):e3901.

Chen TM, Blasco J, Alzubi J, Alzubi O. Intrusion detection. IET Eng Technol Ref 2014;1(1):1–9.

Gheisari M, Bagheri A. Shd: a new sensor data storage. Proceedings of the fifth international symposium on advances in science & technology, 2011.

Gheisari M. Design, implementation and evaluation of SemHD: a new semantic hierarchical sensor data storage. Indian Journal of Innovations and Developments 2012:115–20.

Gheisari M, Wang G, Bhuiyan MZA. A survey on deep learning in big data, 2; 2017. p. 173–80.

Gheisari M, Wang G, Chen S. Iot-SDNPP: a method for privacy-preserving in IoT-based smart city with software defined networking. Proceedings of the 18th international conference on algorithms and architectures for parallel processing. Springer, 2018.

Gheisari M, Wang G, Chen S. An edge computing-enhanced IoT architecture for privacy-preserving in smart city. Comput Electr Eng 2019;6:77265–71.

Jafari M, Wang J, Qin Y, Gheisari M, Shahabi AS, Tao X. Automatic text summarization using fuzzy inference. In: Proceedings of the 2016 22nd international conference on automation and computing (ICAC); 2016. p. 256–60.

Kalkan K, Zeadally S. Securing internet of things with software defined networking. IEEE Commun Mag 2018;56(9):186–92. doi:10.1109/MCOM.2017.1700714.

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.

Liu Q, Guo Y, Wu J, Wang G. Effective query grouping strategy in clouds. J Comput Sci Technol 2017a;32(6):1231–49.

Liu Q, Wang G, Li F, Yang S, Wu J. Preserving privacy with probabilistic indistinguishability in weighted social networks. IEEE Trans Parallel Distrib Syst 2017b;28(5):1417–29.

Liu Q, Wang G, Liu X, Peng T, Wu J. Achieving reliable and secure services in cloud computing environments. Comput Electr Eng 2017c;59:153–64.

M A, M G, A H. An improved node scheduling scheme for resilient packet ring network. Majlesi J Electr Eng 2015;9(2):43.

M G, G W, MDZA B, Z W. Mapp: a modular arithmetic algorithm for privacy preserving in IoT. In: Proceedings of the 2017 IEEE international conference on ubiquitous computing and communications (ISPA/IUCC), 2017 IEEE international symposium on parallel and distributed processing with applications. IEEE; 2017. p. 897–903.

Mehdi Gheisari Guojun Wang SCAS. A method for privacy-preserving in IoT-SDN integration environment. Proceedings of the 16th IEEE international Symposium on parallel and distributed processing with applications (ISPA 2018). Melbourne, Australia, 2018.

M.Gheisari, M.Esnaashari. Data storages in wireless sensor networks to deal with disaster management. In: Proceedings of the emergency and disaster management: concepts, methodologies, tools, and applications. IGI Global; 2019. p. 655–82.

Nazir S, Hamdoun H, Alzubi J. Cyber attack challenges and resilience for smart grids. Eur J Sci Res 2015;134.

Papadimitriou CH. Computational complexity. John Wiley and Sons Ltd.; 2003.

Peng T, Liu Q, Wang G. A multilevel access control scheme for data security in transparent computing. Comput Sci Eng 2017;19(1):46–53. doi:10.1109/MCSE.2017.13.

Peng Z, Wang G. An optimal energy-saving real-time task-scheduling algorithm for mobile terminals. Int J Distrib Sensor Netw 2017;13(5) 1550147717707891.

Rezaeiye P, pp Rezaeiye, Beig EFGM, Mohseni H, Kaviani R, Gheisari M, Golzar M. Agent programming with object oriented (C++). In: Proceedings of the 2017 second international conference on electrical, computer and communication technologies (ICECCT). IEEE; 2017. p. 1–10.

Sethuraman J, et al. Eccentric methodology with optimization to unearth hidden facts of search engine result pages. Recent Pat Comput Sci 2019;12(2):110–19.

Sharma PK, Singh S, Jeong Y, Park JH. Distblocknet: a distributed blockchains-based secure SDN architecture for IoT networks. IEEE Commun Mag 2017;55(9):78–85. doi:10.1109/MCOM.2017.1700041.

United Nations New York NDoE, Affairs S. World population ageing, 1950-2050. United Nations Publications; 2002.

Wang F, Li J, Jiang W, Wang G. Temporal topic-based multi-dimensional social influence evaluation in online social networks. Wirel Pers Commun 2017;95(3):2143–71.

Wang G, Liu Q, Wu J, Guo M. Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers. Comput Secur 2011;30:320–31.

Wang G, Zhou W, Yang LT. Trust, security and privacy for pervasive applications. J Supercomput 2013;64:661–3.

Wang T, Bhuiyan MZA, Wang G, Rahman MA, Wu J, Cao J. Big data reduction for a smart city's critical infrastructural health monitoring. IEEE Commun Mag 2018;56:128–33.

Yari G, Rahimi M, Kumar P. Multi-period multi-criteria (MPMC) valuation of american options based on entropy optimization principles. Iran J Sci Technol Trans A: Sci 2017;41(1):81–6.

Yu S, Wang G, Zhou W. Modeling malicious activities in cyber space. IEEE Netw 2015;29(6):83–7.

Zhang Q, Liu Q, Wang G. PRMS: a personalized mobile search over encrypted outsourced data. IEEE Access 2018;6:31541–52.

Zhang Q, Wang G, Liu Q. Enabling cooperative privacy-preserving personalized search in cloud environments. Inf Sci 2019;480:1–13.

Zhang S, Wang G, Liu Q. A dual privacy preserving scheme in continuous location-based services. In: Proceedings of the 2017 IEEE Trustcom/BigDataSE/ICESS; 2017a. p. 402–8.

Zhang S, Wang G, Liu Q, Abawajy JH. A trajectory privacy-preserving scheme based on query exchange in mobile social networks. Soft Comput 2017b;22:1–13.

Zhang S, Wang G, Liu Q, Abawajy JH. A trajectory privacy-preserving scheme based on query exchange in mobile social networks. Soft Comput 2018;22(18):6121–33.

Mr. Mehdi Gheisari is a Ph.D. Candidate in computer science. 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 department of computer science. Mr. Gheisari did his Masters of computer software engineering from Islamic Azad university and Amirkabir University. There, he worked on data storage of Wireless Sensor Networks. He proposed an effective method for data storage in WSNs. Prior to that, he did his B.Sc. in software engineering from Islamic Azad University, Iran where he worked on design and implementation of automation. Provided with strong background, Mr. Gheisari has research interests in Privacy-preserving in IoT, WSNs, Big Data, Deep Learning. Mehdi Gheisari has gained a wealth of knowledge in dealing with Publishing articles. The research results have been published in ranked journals (such as IGRDJ, INDJST, etc) and in many highly ranked conferences (such as IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD 2016), ISPA, UIC, EUC, ICCSET Switzerland, Zurich and so on). His profile can be accessed via: https://scholar.google.com.sg/citations?user=tmWQt9UAAAAJ&hl=en