2017 IEEE International Symposium on Parallel and Distributed Processing with Applications and 2017 IEEE International Conference on Ubiquitous Computing and Communications (ISPA/IUCC)

MAPP: A Modular Arithmetic Algorithm for Privacy Preserving in IoT

Mehdi Gheisari[†], Guojun Wang[*][†], Md Zakirul Alam Bhuiyan[‡], and Wei Zhang[†]
[†]School of Computer Science and Educational Software, Guangzhou University, Guangzhou, China, 510006
[‡]Department of Computer and Information Sciences, Fordham University, New York, NY, 10458
[*]Correspondence to: csgjwang@gzhu.edu.cn

***Abstract*—High-speed Internet becomes more widely accessible, the cost of connecting devices is reducing, more devices are being created with Wi-Fi abilities and sensors are built into those devices, technology costs are cost-effective. All of these things are creating a "storm" for the Internet of Things (IoT) era. With the emergence of the Internet of Things, connect things through internet, there are many devices that are providing data. The more devices, the more data. If these devices want to share data with the aim of achieving abstract knowledge, they need to pass through the network. Some devices provide sensitive information that can be time. We should protect these sensitive data, from unwanted disclosure that is called privacy. In other words, privacy preserving of data is one of the main problems of IoT devices, protecting sensitive data against unauthorized users when we do analysis and even transferring data. To achieve this in this paper, we propose a new method based on modular arithmetic for privacy-preserving when IoT devices produce sensitive time label called MAPP. We applied Number Theory, Modular Arithmetic to achieve that aim. We used CupCarbon 3.0 for simulation and evaluating our proposed method. Performance evaluation shows that our proposed method has good performance from the energy consumption point of view.**

***Index Terms*—Privacy-Preserving Data Publishing, IoT, CupCarbon, Internet of Things, Data Publishing, Privacy Preserving Data Mining.**

I. Introduction

In the comprehensive sense, the term IoT includes everything is connected to the internet, but it is commonly being used to define objects that "talk" to each other. "Simply, the Internet of Things is made up of devices from simple sensors to smart phones and wearable ones connected together" [5]. In brief, Internet of Things means connecting digital devices with each other through a network. Based on approximation the number of these digital devices will be increased to 50B until 2020 [20]. Each of these devices produces data. The huge number of IoT devices along with data produced by them during time bring new challenges such as privacy of data, data privacy, and context privacy, that means the right of anyone to keep his personal information hidden with the aim of no one will be able to interfere [18]. How to publish data that contains sensitive information of individuals has received significant consideration in recent years. Types of sensitive data are:

1) Personal: same as Name, Social Secure Number
2) Sensitive data: Same as Salary and Disease
3) Quasi Identifier: Same as Age, Zip code

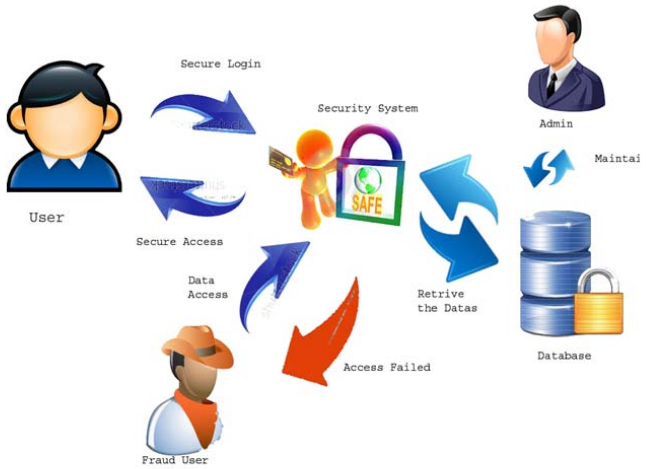


Fig. 1. Role of fraud user, security, and privacy

Why Quasi identifier is important and it is a type of sensitive data? Because with the help of those we can uniquely identify individuals from joining them with the combination of information gotten from diverse external sources (e.g., public voting registration data) to re-identify the individuals in the published data. Fig. 1 shows the privacy issue in schematic form.

Fig. 1 shows the privacy conception, in general, and also shows a situation that a user wants to send data and stores them in the database but a fraud user wants to access data without proper authorization so we have to provide a proper way in order to whenever fraud user wants to access data he will face with inaccurate data. In other words, we have to provide users a way to send and receive data in order to no one can find the original data when we are faced with external adversaries or internal adversaries. So we have to deal with this important issue of privacy preserving in IoT devices.

The major contribution of this paper is two-fold:

1) We formulate the problem of privacy-preserving issue in IoT, and we classify privacy preserving dimensions.
2) We also propose a novel method for privacy-preserving in IoT environment that is able to process sensors data without disclosing sensitive information. In brief, we propose an algorithm for data analysis of the IoT devices

0-7695-6329-5/17/31.00 ©2017 IEEE
DOI 10.1109/ISPA/IUCC.2017.00137

meanwhile protecting data against the public publishing of them without any authorization. The proposed algorithm is based on modular algorithm. Each IoT device sends its data after modulating its data to the server. Then the server demodulates received data in order to perform data aggregation.

This paper is organized as follows. In Section 2, we discuss related work. Section 3 describes problem formulation, provides some information about IoT, network model, and data privacy preserving that is time. Section 4 pays attention to privacy preserving in IoT environment. Section 5 indicates our proposed algorithm procedure for privacy preserving in IoT environment. Section 6 we simulate and discuss our proposed method. Finally, Section 7 concludes the paper.

II. Related Work

Each IoT device that can be cell phones, sensors, self-driving automobiles, and so on is producing data during the time. These data should remain safe from unrelated access. For achieving this aim, some of the proposed methods that can be applied in IoT environment are listed as follows: In [24], authors proposed an efficient algorithm for privacy-preserving data aggregation based on the secret key of each participant. But it has a drawback that is, when there is a malfunctioning device in the system, aggregated data is not able to be recovered correctly. In another word, this scheme is not fault-tolerant. [11] Used homographic Paillier encryption with the aim of better aggregation that can also keep privacy-preserving. Without their restrictions, their method is fault tolerant. In 2012, authors in [17] used the encryption method based [9] with the aim of presenting an efficient method that is a lightweight one. But it did not consider the fault-tolerance problem. Chan et al in [13] presented mechanisms, improved scheme [11], with applying new mechanisms, the new scheme is resilient to failures and compromises. A privacy-preserving multi-dimensional data aggregation method called EPPA was introduced in [7] that combined both Paillar encryption and increasing sequence techniques, can reduce communication overhead but it has multiple time-consuming exponential computations problem. In [27], authors presented multi function in a branch of IoT, smart grid communication, based on Boneh-Goh-Nissim (BGN) encryption homomorphic method [26] which can support average, variance. Authors in [3] used a lattice cryptographic method to show a dual function aggregation privacy-preserving method that is able to support mean and variance functions simultaneously. Authors in [17], [14], [1], [19], [16], [4] proposed novel aggregation algorithms that took into consideration fault tolerance, data integrity, and differential privacy.

III. Problem Formulation

At first, we will have a look at the network model that we want to simulate then privacy preserving in time dimension.

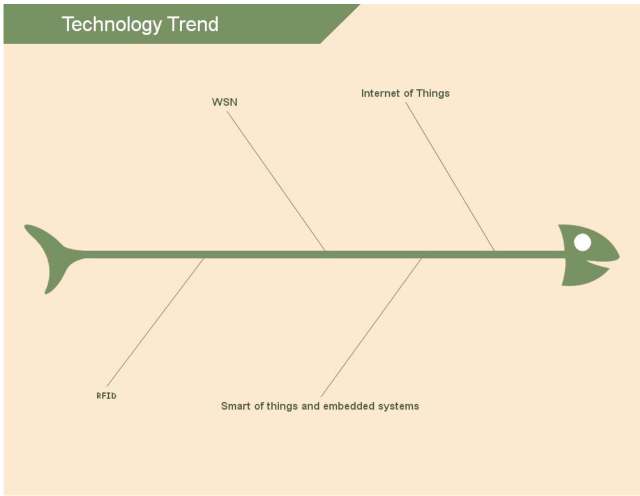


Fig. 2. Technology evolution from 2000

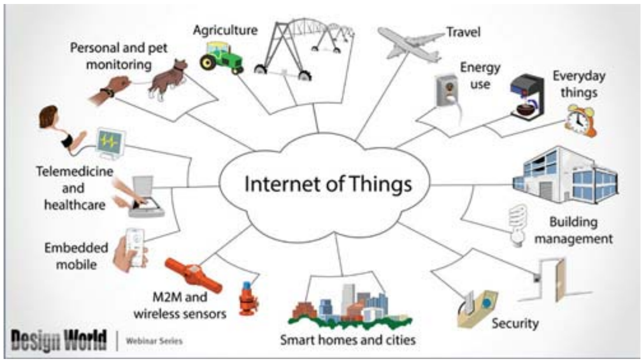


Fig. 3. IoT environment, connecting variety of domains [10]

1) Network Model: IoT in simple means connecting machines and devices with each other in order that they collaborate with each other to provide better services [23]. From another point of view, Internet of Things means connecting things with each other over a network without human-to-machine or human-to-computer interactions. Things can be a person to monitor implant, automobiles with sensors or even any handicraft that can have a unique identifier or IP and they should have the ability to send their data over the network. IoT can change our lifestyle hugely. So we have to deal with its challenges. Most of these Things are sensors that are limited in energy. So we have to consider this energy parameter limitation. Fig. 2 shows the trend of technology from 2000 till 2017.

Fig. 2 shows the trend of advancement of technology after the creation of RFID [22] until the IoT step by step. The trend is that at first RFID was created, then based on RFID, wireless sensor networks(WSNs)were created. Next smart things and embedded systems. At last, today, we are facing with IoT area.

As Fig.3 shows in IoT environment, each device is disseminating its data in wireless mode in order to collaborate with

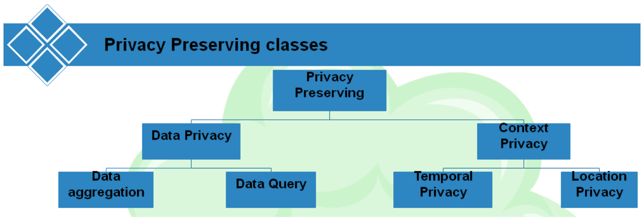


Fig. 4. Privacy Preserving clasess in IoT

other devices with the aim of providing better services with the help of using and analyzing other's data.

A. *Privacy Preserving in Time*

In some applications of IoT, we need to protect the sensed value that is time so that no one can understand the data of IoT devices. One major example of time privacy preserving is in the mobile targeting because the adversary with the knowledge of timing information is able to find the real location of the target that stems from private information leakage. Devices share their data in order to use others data so they have to be more careful about the privacy of their data [8]. So we have to investigate about how we can apply privacy-preserving algorithms [29]. The two major differences between traditional sensors and IoT objects are computing capabilities and the ability to install applications of third-parties that IoT devices can support.

IV. Privacy Preserving in IoT

Privacy-preserving means not disclosing information via legitimate tools in reverse of security. In other words, the difference between Privacy and Security is that Privacy preserving is achieved through legitimate access, but security via illegitimate such as hacking, query injection and so on. If we want to categorize how we can keep privacy in IoT environment, we can pay attention to two main classes as Fig.4 shows:

Privacy in IoT can be divided into two main classes: Data privacy and context privacy. Data privacy means how to protect individual data from disclosing information without right that can be divided into two sub-branches: Data Aggregation and Data Query. Privacy-preserving in data aggregation means doing the aggregation of IoT devices data using its corresponding methods without disclosing sensitive information. Privacy-preserving in Data Query means how to process users query for data in private mode and context-oriented pay attention to contextual information such as location and timing of traffic flow in the network. Fig.5 shows the privacy preserving in IoT environment.

Fig.5 shows data consumers or users need to access data from a variety of devices such as Vanets [11], WBSN (Wireless Body Sensor network) [17], Embedded systems [12]. These data should be transmitted in a way that sensitive data should remain private in order to non-authorized person would not be able to access original data. There are two types of attacks from high-level perspectives that are:

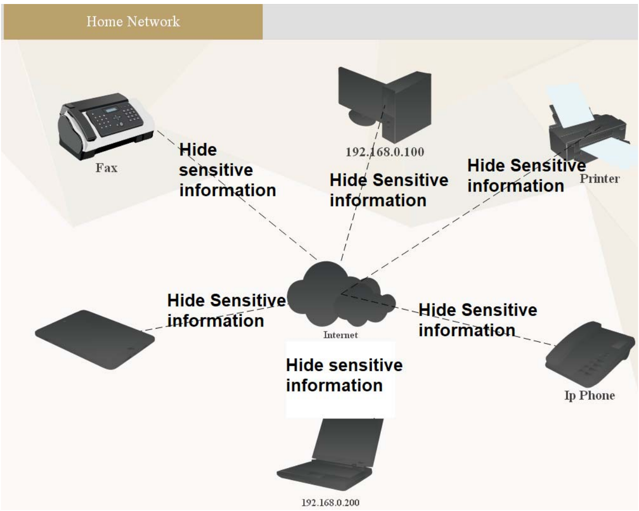

Home Network
Fax
Hide sensitive information
192.168.0.100
Hide Sensitive information
Hide Sensitive information
Printer
Hide Sensitive information
Internet
Hide Sensitive information
Hide sensitive information
Ip Phone
192.168.0.200

Fig. 5. Privacy Preserving in IoT

1) Internal: Means some of IoT devices can be malicious parties that lead to misleading information so that we must propose mechanisms in order to find internal attacks and addressing them.
2) External: Means attacking from outside of the system not local. If we want to deal with external attack, one common method is using cryptography algorithms.

A. *Assumptions*

In this subsection, we pay attention to assumptions that we consider are applied to the network.

- IoT devices are spread in smart city.
- The attack that we have to cope with is external attack.

B. *PPDP in IOT*

The aim of this section is formulating why we need PPDP (Privacy-Preserving Data Publishing) and introducing a novel algorithm that can preserve time data privacy of IoT devices when they want to share data [28].

1) Why do we need PPDP in IOT: With the help of Data Publishing (DP) algorithms, we can publish data into public without been worried about the privacy of data that in our current scenario is time . Each IoT device sends its data into an environment called Cloud [2] for further processing and analyzing their data in Cloud. Each sensor can share its data with other related sensors in order to provide better services so that we can apply DP algorithms. But the problem is that when we want to apply DP, any third party that can access data is able to find sensitive information such as personal identity. So we have to propose some mechanisms that no one can understand the original sensitive data when we want to publish them to the public.

2) PPDP approaches: In this section, we classify current approaches in privacy-preserving domain.

1) Data anonymization: Can be achieved via generalization, data removal, swapping and condensation, and so on.

Condensation means creating limited clusters then generating some data based on the statistic of those clusters.

2) Data Perturbation: Means disclosing perturbed data rather than original one before of publishing data. Data perturbation can be applied to both centralized and distributed environments. We also can add noise from a known distribution into the dataset. Another method for data perturbation is data swapping. A traditional perturbation technique is Randomization, randomly change data values [15].
3) Data Randomization: Altering data by adding a noise component extracted from a discrete probability distribution that can be categorized into two main classes: numerical randomization and item set randomization same as data swapping across different records [6].
4) Cryptography: Cryptography is the science of secret writing is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. when an Egyptian scribe used non-standard hieroglyphs in an inscription. Some experts debate that cryptography appeared suddenly sometime after writing was created, with applications ranging from diplomatic missives to war-time battle plans. It is no surprise, then, that new forms of cryptography came soon after the prevalent development of electronics and computer communications. In data and telecommunications, cryptography is compulsory when cooperating over any untrusted medium, which includes just about any network, particularly the Internet [25]. Basically, there are five functions of cryptography today that can be applied:
    - Privacy/confidentiality: Ensuring that no one can read the message except the intended receiver.
    - Authentication: The process of proving one's identity.
    - Integrity: Assuring the receiver that the received message has not been altered in any way from the original.
    - Non-repudiation: A mechanism to prove who really sent the message, real sender or fake one.
    - Key exchange: Methods by which crypto keys are shared between sender and receiver.

3) PPDP metrics for evaluation: The criteria that we can use for measurement of different algorithms and compare them are:

- Accuracy: amount of information loss
- Completeness and consistency: degree of unused data in the original dataset.
- Scalability: the increase of performance when the number of parties will be increased.

V. MAPP:PROPOSED METHOD

For simulating and evaluating MAPP, we have to pay attention to some background information such as the definition of Modular Arithmetic, and why it is useful.

A. Modular Arithmetic

The rules Modular Arithmetic (mod) or clock arithmetic, In a clock, there are 12 hours, and once you get to 12:00, the next hour starts again at 1:00. In modular arithmetic, 12 would be called the modulus or the number we start over at. In brief, R mod N is equal to the remainder when we divide R by N, and the rules of addition, subtraction, and multiplication in modular arithmetic are as follows:

- If a + b = c, then (a + b) mod n is equal to c mod n.
- If a mod n is equal to d mod n and b mod n is equal to e mod n, then (a + b)mod n is congruent to d mod n + e mod n.

In both of these rules, the plus sign can be replaced by a subtraction or multiplication sign. These rules describe what we can first do the operation and then calculate that number mod n, or we can calculate each of the numbers mod n and then perform the operation on them. It is important to note that when we addressing with subtraction, we may get negative numbers. When this happens, we have to add multiples of the modulus n until when we get a number between 0 and n. Suppose mm be any natural number, and let a,b,c,da,b,c,d be any integers. Then: modulo mm is an equivalence relation. That is, aa mod maa mod m. If ab mod mab mod m, then ba mod mba mod m. If ab mod mab mod m and bc mod mbc mod m, then ac mod mac mod m. Addition and multiplication are well-defined modulo mm. That is, If ab mod mab mod m and cd mod mcdmodm, then a+cb+d mod ma+cb+d mod m, and acbdmod macbd mod m. If acbc mod mcacbc mod mc, then ab mod mab mod m. The congruence axb mod maxb mod m has solutions (i.e., integers xx making the statement true) if and only if gcd(a,m)gcd(a,m) divides bb. You also have If pp is a prime and 1kp11kp1, then the binomial coefficient (pk)(pk) satisfies (pk)0 mod p(pk)0 mod p. Fermat's little theorem, and its generalization, Euler's theorem There are primitive roots modulo mm if and only if m=pkm=pk or m=2pkm=2pk where pp is an odd prime number, or if m=2m=2 or m=4m=4 [21].

What is meant by Mod, Modulus and Modular Arithmetic? Modulus (abbreviated as "mod") is the Latin word for remainder, residue or more in what is left after parts of the whole are taken. Thus, "modular" or "mod arithmetic" is really "remainder arithmetic". More precise: We are looking for the integer that occurs as a remainder (or the "left-over") when one integer is divided by another integer. Example: When 9 is divided by 3 it leaves no remainder. Thus, we write: 9 mod 3 = 0 [1] .

B. What is the usage of Modular arithmetic

365 MOD 7 = 1 tells us that if Christmas will fall on Thursday and we don't have a leap year it will fall on a Friday next year. The same for your birthday and any other day as well: every weekday will fall on the following weekday the next year [20].

C. Procedure

The procedure of the proposed algorithm is the same as follows:

- At first, each device uses Numerical Theory, Modular Arithmetic part, to change device data in order to keep those time data private. It means that in the first step

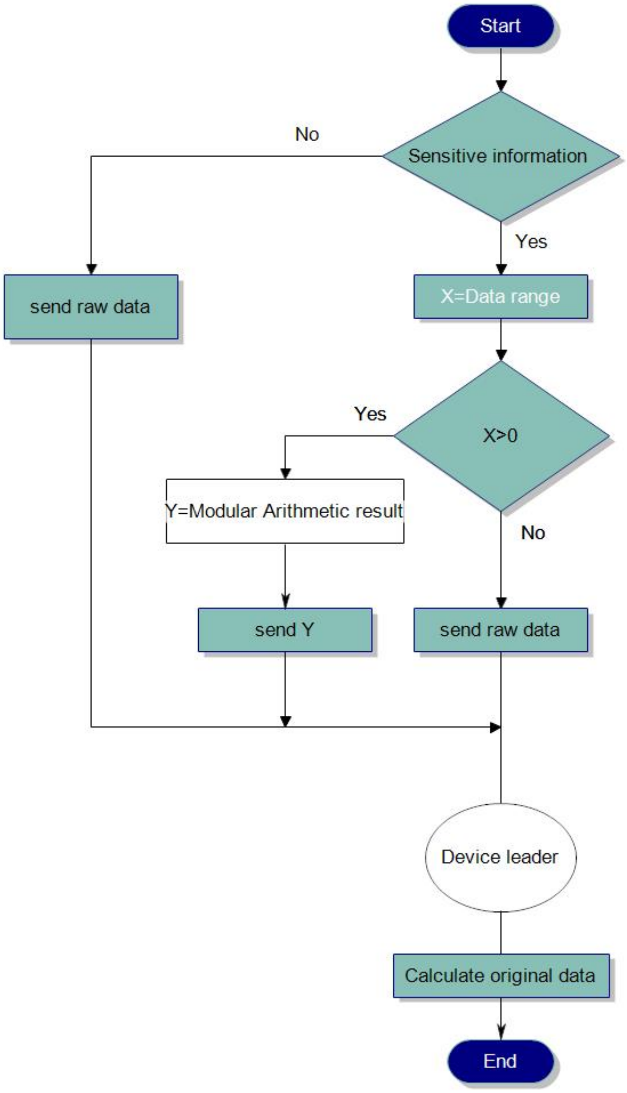


Fig. 6. Flowchart of MAPP

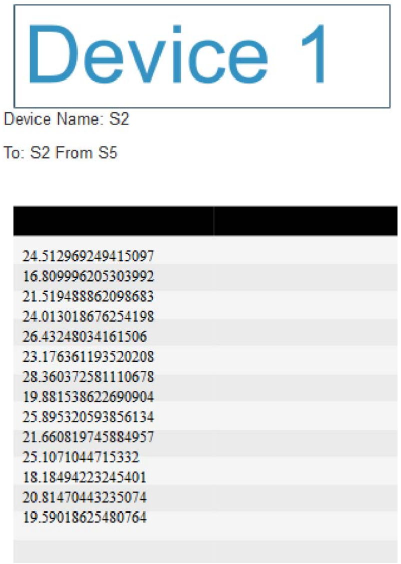
we find the sensor data range of each sensor then we apply the IoT device data range (as a divider) to its data(as a dividend) and we calculate its remainder. Then we consider remainder as new data.

- Each device sends its changed data(new data) to a corresponding device, leader so that it controls all related devices in that area.
- In the leader device, we use the received data of devices.

D. Technical Diagram

Fig.6 shows the technical algorithm of our proposed method in flowchart mode.

The advantage of this method is that if any external attacker wants to find the original data it will not able to that. And the disadvantage is the amount of it's overload.



Device 1

Device Name: S2

To: S2 From S5

```
24.512969249415097
16.809996205303992
21.519488862098683
24.013018676254198
26.43248034161506
23.176361193520208
28.360372581110678
19.881538622690904
25.895320593856134
21.660819745884957
25.1071044715332
18.18494223245401
20.81470443235074
19.59018625480764
```

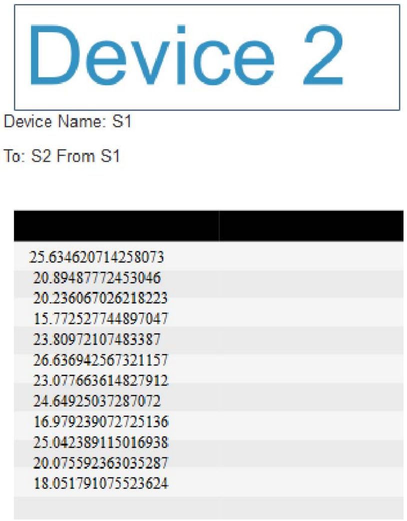
Fig. 7. S2 (Device1) data

VI. SIMULATION AND DISCUSSION

We simulate a privacy-preserving method in IoT environment based on modular algorithm technique as its theory and flowchart were described in the previous section. For simulation purpose, we used CupCarbon U-One 3.3 simulator that is a smart city and IoT Wireless Sensor Network Simulator that is a part of the research project PERSEPTEUR supported by the French research agency ANR (Agence Nationale de la Recherche) under the reference ANR-14-CE24-0017-01. It's objective is to design, debug and validate distributed algorithms for monitoring, environmental data collection, so on, and to create environmental scenarios such as fires, gas, mobiles, and generally within educational and scientific projects. Not only it can help to visually explain the basic concepts of sensor networks and how they work; it may also support scientists to test their wireless topologies, protocols, and so on. At first IoT device senses following values during the time that we should keep them private is shown in Fig.7. These data are generated in 23 seconds as our simulation runtime.

Fig. 8 shows the second IoT device data.

In more detail, Fig. 7 and 8 shows sensed IoT data. We hide sensitive time data based on the Number Theory. We assume that both of IoT devices produce sensitive data so that no one will be able to understand the real sensitive data. Each transmitter, IoT device, sensed a time data, perturbs it's data. Next, they send their perturbed data to leader device for further analysis such as classification purpose. The simulation time is 23 seconds. Fig. 9 shows the simulation environment in abstract level. From another point of view, we simulate three IoT devices that two of them send it's data to a leader device for further analysis in a smart city environment. And the IoT device leader will aggregate those received data using data



Device 2

Device Name: S1

To: S2 From S1

25.634620714258073	
20.89487772453046	
20.236067026218223	
15.772527744897047	
23.80972107483387	
26.636942567321157	
23.077663614827912	
24.64925037287072	
16.979239072725136	
25.042389115016938	
20.075592363035287	
18.051791075523624	

Fig. 8. S5 (Device2) data

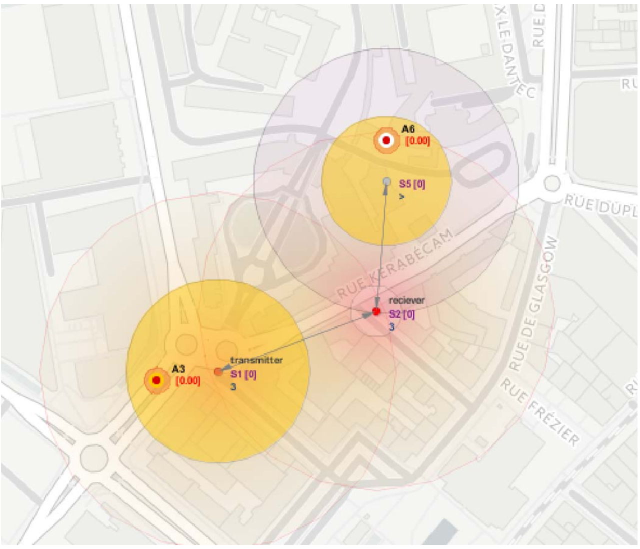


Fig. 9. Simulation environment

classification algorithm. Meanwhile, we have to preserve data private.

As Fig. 9 shows, we put three sensors in different parts of a block in a smart city environment(S1, S2, S5). The device leader is S2. The red points (A3 and A6) show the exact place of sensing areas. And the yellow more colorful areas show the domain range of sensing areas. Each one senses data and encrypts its sensitive data. Next, they will send to the IoT leader. Then leader decrypts received IoT data. Fig. 10 shows the simulation result of the above scenario from energy consumption point of view.

Simulation result shows the remaining energy of each sensor. The X-axis shows the time in second and Y-axis shows the remaining energy of each sensor based on the Joule. As

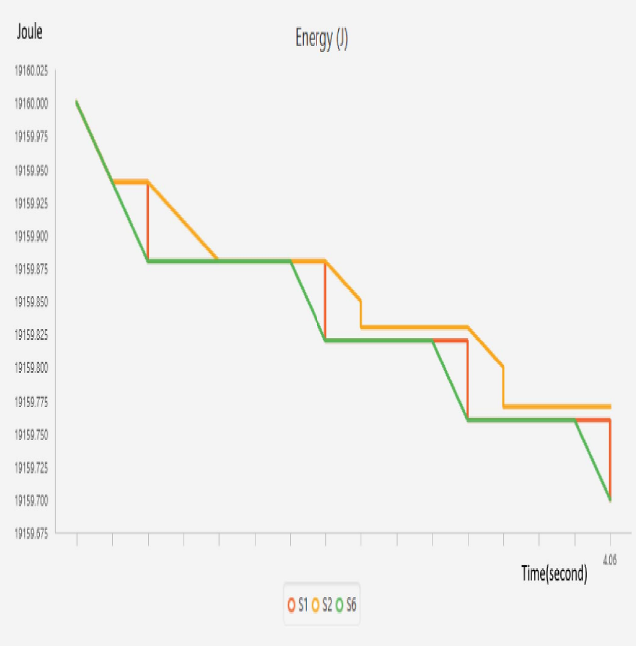


Fig. 10. Energy consumption of proposed method

the result shows the energy consumption of the IoT device leader, S6, is higher than others, but we achieve more privacy and we protected private data so that no one finds true data without having rights. For example, in time 1.5, each sensor has the same energy that is 19159.875 joule. But the energy consumption of the leader during time is more than others.

VII. Conclusion and Future Work

The Internet of Things is the idea of everyday objects from industrial machines to wearable devices using integral sensors to gather data and take action on that data using actuators. Each object talks with others in order to provide better services. Until 2020 experts estimate that the Internet of Things (IoT) will enable device to device communication for 50 billion objects. It's aim is visualizing the potential of all those connections for smart phones, smart vehicles, smart appliances, smart power grids and smart medical devices. In our connected future, a majority of organizations remains disconnected from the opportunities that it offers because of privacy issue. So we have to research on how we can use IoT environment without disclosing sensitive information to others. Sensitive data can also be times of sensing so that we have to protect it. One possible solution for privacy-preserving (protecting sensitive information from disclosure without right) in IoT environment is that each device can apply privacy-preserving algorithms in order to achieve both privacy and doing analyses. One of privacy-preserving algorithm that hides the time of IoT device is presented in this paper. One of future work is simulating and implementing this algorithm with more details that can be verifiable as if it is scalable or not and also the amount of overhead. Another future work is comparing this algorithm with other related algorithms.

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] "Cryptography tutorial - modular arithmetic," https://www.ti89.com/cryptotut/modarithmetic.htm, (Accessed on 10/22/2017).

[2] "Overview of internet of things — solutions — google cloud platform," https://cloud.google.com/solutions/iot-overview, (Accessed on 10/22/2017).

[3] V. Atluri, *Data and Applications Security XXII: 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security London, UK, July 13-16, 2008, Proceedings*. Springer, 2008, vol. 5094.

[4] S. M. H. Bamakan, H. Wang, and Y. Shi, "Ramp loss k-support vector classification-regression; a robust and sparse multi-class approach to the intrusion detection problem," *Knowledge-Based Systems*, vol. 126, no. Supplement C, pp. 113 – 126, 2017. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0950705117301314

[5] M. Z. A. Bhuiyan, T. Wang, T. Hayajneh, and G. M. Weiss, "Maintaining the balance between privacy and data integrity in internet of things," in *Proceedings of the 2017 International Conference on Management Engineering, Software Engineering and Service Sciences*, ser. ICMSS '17. New York, NY, USA: ACM, 2017, pp. 177–182. [Online]. Available: http://doi.acm.org/10.1145/3034950.3035011

[6] C. Cadar, P. Akritidis, M. Costa, J.-P. Martin, and M. Castro, "Data randomization," Technical Report TR-2008-120, Microsoft Research, 2008. Cited on, Tech. Rep., 2008.

[7] 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 *2016 IEEE 20th International Conference on Computer Supported Cooperative Work in Design (CSCWD)*, May 2016, pp. 174–179.

[8] M. Gheisari, G. Wang, and M. Z. A. Bhuiyan, "A survey on deep learning in big data," in *2017 IEEE International Conference on Computational Science and Engineering (CSE) and IEEE International Conference on Embedded and Ubiquitous Computing (EUC)*, vol. 2, July 2017, pp. 173–180.

[9] M. Gheisari and A. R. Bagheri, "Shd: a new sensor data storage," in *In 5th international symposium on advances in science & technology*, May 2011.

[10] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (iot): A vision, architectural elements, and future directions," *Future generation computer systems*, vol. 29, no. 7, pp. 1645–1660, 2013.

[11] C. B. H. Hasrouny, A. E. Samhat and A. Laouiti, "Vanet security challenges and solutions: A survey," *Veh. Commun.*, ol. 7, pp. 720, Jan. 2017.

[12] T. A. Henzinger and J. Sifakis, "The embedded systems design challenge," in *Proceedings of the 14th International Conference on Formal Methods*, ser. FM'06. Berlin, Heidelberg: Springer-Verlag, 2006, pp. 1–15. [Online]. Available: http://dx.doi.org/10.1007/11813040_1

[13] M. Jafari, J. Wang, Y. Qin, M. Gheisari, A. S. Shahabi, and X. Tao, "Automatic text summarization using fuzzy inference," in *2016 22nd International Conference on Automation and Computing (ICAC)*, Sept 2016, pp. 256–260.

[14] H. Kargupta, S. Datta, Q. Wang, and K. Sivakumar, "On the privacy preserving properties of random data perturbation techniques," in *Third IEEE International Conference on Data Mining*, Nov 2003, pp. 99–106.

[15] ——, "Random-data perturbation techniques and privacy-preserving data mining," *Knowledge and Information Systems*, vol. 7, no. 4, pp. 387–414, May 2005. [Online]. Available: https://doi.org/10.1007/s10115-004-0173-6

[16] M. F. Khan and B. Wang, "Effective placement of femtocell base stations in commercial buildings," in *2014 Sixth International Conference on Ubiquitous and Future Networks (ICUFN)*, July 2014, pp. 176–180.

[17] X. Lai, Q. Liu, X. Wei, W. Wang, G. Zhou, and G. Han, "A survey of body sensor networks," *Sensors*, vol. 13, no. 5, pp. 5406–5447, 2013. [Online]. Available: http://www.mdpi.com/1424-8220/13/5/5406

[18] X. Li, Z. Yan, and P. Zhang, "A review on privacy-preserving data mining," in *2014 IEEE International Conference on Computer and Information Technology*, Sept 2014, pp. 769–774.

[19] K. Mehdi, M. Lounis, A. Bounceur, and T. Kechadi, "Cupcarbon: A multi-agent and discrete event wireless sensor network design and simulation tool," in *Proceedings of the 7th International ICST Conference on Simulation Tools and Techniques*, ser. SIMUTools '14. ICST, Brussels, Belgium, Belgium: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2014, pp. 126–131. [Online]. Available: https://doi.org/10.4108/icst.simutools.2014.254811

[20] M. G. Mehdi Gheisari, Hamed Baloochi and M. Khajehyousefi., "An evaluation of two proposed systems of sensor datas storage in total data parameter,," *International Geoinformatics Research and Development Journal*, March 2012.

[21] S. Ovshinsky and B. Pashmakov, "Methods of factoring and modular arithmetic," Mar. 30 2004, uS Patent 6,714,954. [Online]. Available: https://www.google.com/patents/US6714954

[22] M. S. H. M. Payam Porkar, Mojtaba Fazli and M. Gheisari., "Sensor networks challenges," in *In 11th international conference on data networks, DNCOCO '12*, 7-9 September, 2012.

[23] M. S. Rahman, A. Basu, and S. Kiyomoto, "Privacy-friendly secure bidding scheme for demand response in smart grid," in *2015 IEEE First International Smart Cities Conference (ISC2)*, Oct 2015, pp. 1–6.

[24] P. S. S. Parmar and P. Gupta, "A coherent technique for privacy preservation in data mining using classification," *Sheryl Parmar Preeti Gupta Computer Science*, no. 2277, pp. 642644, 2015.

[25] D. R. Stinson, *Cryptography: theory and practice*. CRC press, 2005.

[26] L. Sweeney, "k-anonymity: A model for protecting privacy," *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, vol. 10, no. 05, pp. 557–570, 2002.

[27] J. S. Vaidya, "Privacy preserving data mining over vertically partitioned data," in *Thesis, India*, no. August, 2004.

[28] L. Yang, A. Humayed, and F. Li, "A multi-cloud based privacy-preserving data publishing scheme for the internet of things," in *Proceedings of the 32Nd Annual Conference on Computer Security Applications*, ser. ACSAC '16. New York, NY, USA: ACM, 2016, pp. 30–39. [Online]. Available: http://doi.acm.org/10.1145/2991079.2991127

[29] X. Zhang and H. Bi, "Research on privacy preserving classification data mining based on random perturbation," in *2010 International Conference on Information, Networking and Automation (ICINA)*, vol. 1, Oct 2010, pp. V1–173–V1–178.