Enhancing the Limitations of Sensing Devices in Internet of Things (IoT) using LBOA Scheme

[1]B. Sunil Kumar [2]*M. Kiran Kumar*

[1] *Associate Professor, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

[2] *PG Scholar, Dept. of Master of Computer Applications, Narayana Engineering College, Gudur.*

Abstract- Secure outsourced aggregation in the Internet of Things (IoT) can solve the problem that sensing devices are limited in energy and bandwidth by outsourcing data aggregation task to a third-party service provider. Location-based secure outsourced aggregation (LBOA), aggregating data whose location satisfies user's location strategy, is very important in some location-critical scenarios (e.g., smart homes, intelligent transportation, and smart city). Recent work studied secure data aggregation to reduce transmission overhead and network bandwidth by optimizing topology of networks or adopting the cryptographic approach. However, as far as we know, scarcely any work considers the location information of the data source and the privacy protection of the data at the same time in the studies of secure out source daggregation. In this project, we first propose an LBOA scheme LBOA Max,which can return the maximum value of sensory data whose location satisfies location strategy by applying one-way chain, order-preserving encryption, and some other cryptographic operation. Then, we proposed scheme LBOATop−k and scheme LBOA Sum, which can return the largest k values of data and the summation value of data based on location, respectively. The security analysis results show that our schemes can satisfy the defined requirements and the experiment results show that our schemes are feasible and efficient for each entity in practice.

Keywords:Location-Based,SecureAggregation,CloudComputation,PrivacyProtection,One-WayChain, Order-Preserving Encryption.

1. INTRODUCTION

With the continuous development and improvement of wireless network technology [1], IoT has been more and more widely used in our life [2]. For example, in smart homes [3], smart devices are connected to the external service through the network of IoT, realizing interaction between external service and smart devices. In the field of electronic medical system [4], patients' vital signs such as heart rate and blood pressure can be monitored by wearable devices. IoT is also widely used in intelligent transportation, environmental monitoring, military and many other fields.

However, sensing devices in IoT are usually limited in energy and bandwidth [5], and their computation and storage power are limited. What's more, in general, data requester can not interact with sensing devices directly in IoT. Outsourcing [6]–[8] data aggregation task to a third service provider such as aggregator in cloud [9], [10]-[11] is an effective way to solve the above problems.

Most of the existing work related to secure data aggregation has not considered the location of data source. However, location-based secure outsourced aggregation, i.e. securely aggregate data under location strategy, is very important in some location-critical scenarios. In many IoT applications, the data collected by the sensing device is closely related to the location information of the sensing device [12].For example, in intelligent transportation, the location-critical data sensed by smart devices is one of the most important elements for monitoring, analyzing and forecasting road conditions. In smart homes, the location of data source plays an important role. In applications such as geographic key distribution [13] and geographic routing [14], the smart devices' location also plays a crucial role. Energy productivity is an indicator of the amount of economic output that is derived from each unit of energy consumed [15] [16].

Therefore, a location-based secure outsource daggregation scheme is necessary in IoT to realize aggregating data based on devices' location. Due to the reason that Max, Top-k and Sum are some of the most basic operations of data. Thus, we try to construct location-based secure outsourced aggregation schemes in which aggregator only aggregates data whose location is at the specified position and return the Max or Top-k or Sum value to data requester. However, this work is very challenging [17]. First, it is a challenging task to achieve location-based in IoT because the traditional methods to determine location is not efficient and not suitable to IoT. Second, it is difficult to protect data confidentiality against outside attacker and untrusted aggregator while aggregator needs to aggregate data and return the aggregated result to data requester. Third, it is hard to ensure that aggregator does not have malicious behaviors and guarantee that the user could verify the validity of aggregated result because user cannot get all the raw sensory data in the whole process of aggregation. What's more, the privacy of devices' location and the confidentiality of user's location strategy should also be protected.

Our Contributions

Our contributions in this project are fourfold.

1) We design the system model of location-based secure outsourced aggregation in IoT. Then we propose the threat model. Next, we propose our design goal. The system model of LBOA defines the participants including location-sensitive devices, user and cloud service provider. The system model also defines the participants' task. The threat model in this study describes the adversarial behaviors including data tampering, cheating, data deleting and so on. The design goal of LBOA in this study presents the requirements such as providing service based

on location, achieving location privacy protection, data confidentiality protection and location strategy confidentiality protection.

2) We propose a novel location-based secure outsourced aggregation scheme $LBOA_{Max}$ which can return the maximum value under user's location strategy. Then we propose scheme $LBOA_{Top-k}$ and scheme $LBOA_{Sum}$ which can return the largest k values and the summation value under user's location strategy respectively. Our schemes could aggregate data whose location is at specified location correctly.They could also protect the confidentiality of data and the privacy of the location strategy.

3) We theoretically analyze the security of LBOA. The analysis results show that our schemes satisfy our design goal. At the same time, our schemes support much more data aggregation query operations and are much more secure than existing schemes. 4) We report experimental evaluations of LBOA. The evaluation results show that our schemes are efficient and feasible in practice.

2. RELATED WORK

A. Aggregation

Tan and Körpeoglu proposed a power efficient data gathering and aggregation scheme in wireless sensor networks. Rajagopalan and Varshney introduced data aggregation techniques in sensor networks. Chen et al. presented a data aggregation scheme with distributed randomized algorithms.HekmatandVanMieghemconstructedtheshortest path aggregation tree that maximizes network lifetime. Changand Yen constructed as panning tree based aggregate routing algorithm, selecting the node that performs the data aggregation operation through the coding tree. Lee et al. presented a construct which use geographical route to balance network traffic, and optimize network lifetime and aggregate data rate through optimization methods. However, these data aggregation schemes are mainly concerned with the issue of energy conservation without focusing on the security of data aggregation.

B. Location Verification

Vora and Nesterenko proposed a location verification scheme that can achieve verifying location in-region of provers. Sastry et al. proposed a location verification scheme which can realize verification in a small circular region. Čapkun et al. proposed a scheme which can verify the location through mobile base stations. Sciancalepore et al. proposed a scheme which realize secure location verification by the help of meteor burst communication.

Chandran et al. proposed location-based cryptography in 2009, using user's geographic location information as the user's unique credential. Under BRM model, they proposed secure positioning (SP) protocol which can be proven secure. SP protocol can be used to verify whether the user's location is at the specified location or not. However, SP protocol requires multiple verifiers work together to verify the legitimacy of the location.

Zhang et al. [12] proposed a universally composable secure positioning scheme in the bounded retrieval model. It realized secure location verification. Zhang et al. investigated a scheme which can achieve secure geographical area verification without pre-shared secret. This work is propitious to massive location-critical devices in IoT. All of work above need verifiers to realize location verification. They also require precise time synchronization, and are not robust to computation delay.

C. Location-Based Solution

Kwon et al. [13] proposed a scheme of location-based pairwise key distribution for wireless sensor networks which can achieve perfect resilience and higher connectivity's with less resources. Li et al. [14] proposed an energy efficient cooperative geographic routing scheme in wireless sensor networks which based on sensor nodes' location information. Zhang et al. proposed a position based key exchange scheme which can achieve both security and performance perspectives. Jietal. proposed a blockchain-based multi-level privacy-preserving location sharing scheme which can achieve security and flexibility of location privacy protection. Gao et al. proposed a logistics information privacy protection scheme with position and attribute-based access control which can achieve privacy protection of both logistics information and personal information.

Wang et al.combined data's location with searchable encryption and proposed a secure geometric search scheme on encrypted spatial data. This scheme determined whether the data's location is at specified location or not by executing vector operation which the geometric relationship of the spatial data's location is used. This method of verifying the location of data is very efficient and is suitable to IoT.

3. PROBLEM FORMULATIONS

A) System Model

Thesystemmodeloflocation-basedsecureoutsourcedaggregation (LBOA) is shown in Figure 1.It contains of three entities: user (User), cloud service provider (CSP) and location-sensitive device (LSD).

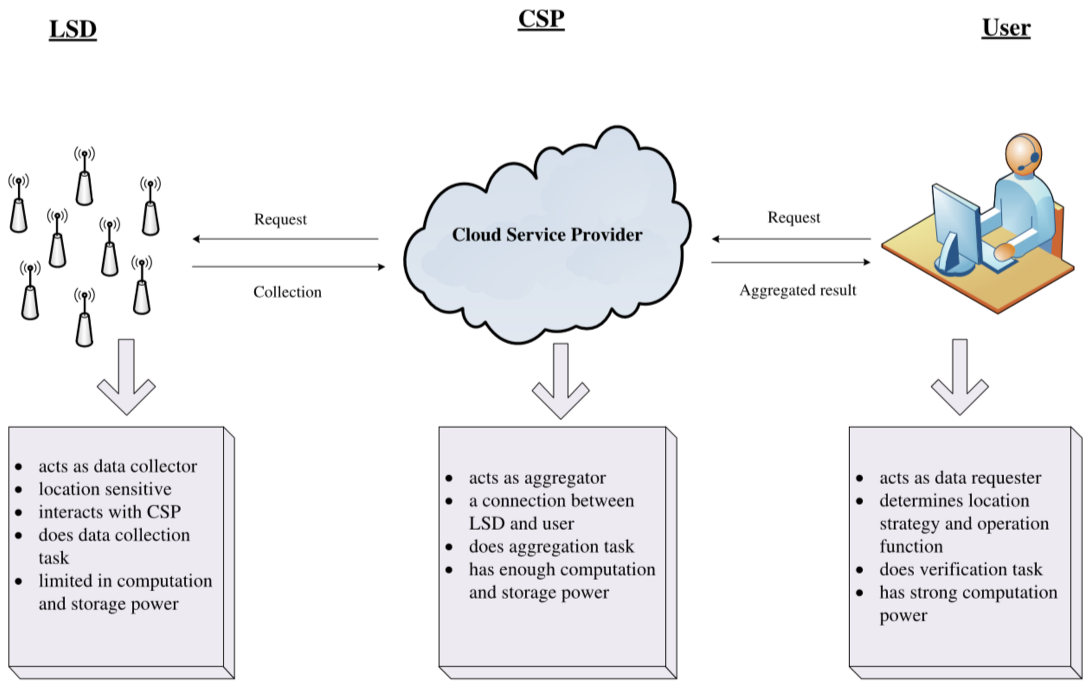

Fig 1. System Model

This system model consists and implements the following modules:

User: User acts as data requester. User determines the location strategy and operation function. He (or she) would like to get LSD's data that satisfying the location strategy and the operation function. However, user cannot interact with LSD directly. Thus, user sends requests to CSP, then CSP aggregates LSD's data and returns aggregated result to user. User will verify the correctness and completeness of the aggregated result after receiving the aggregated result from CSP.

CSP:CSP acts as a connection between location sensitive devices and user. There may be one or multiple aggregators in CSP to do aggregation task. CSP has the ability to do calculation operation and aggregation operation. He (or she) receives data from LSDs and aggregates the data to get an aggregated result, and then sends the aggregated result to user.

LSD:LSD acts as data collector. There are multiple location sensitive devices. Each LSD has a location coordinate. LSD can interact with CSP. LSD may collect sensory data and then outsource data aggregation task to CSP.

B) Design Goal

According to the requirements and the threat model of location-based secure outsourced aggregation, the proposed schemes should satisfy the following design goal:

1) Achieve secure aggregation based on sensing devices' location(LB).Our schemes should realize aggregation based on location. CSP should aggregate data whose location satisfies user's location strategy.

2) Support some basic query operations in aggregation such as Max, Top-k and Sum. Our schemes should achieve returning the Max (Top-k/Sum) value of data under user's location strategy correctly.

3) Guarantee the verifiability of aggregation (AV). Our schemes should guarantee CSP does not tamper the aggregation process. Our schemes should also ensure that the correctness and completeness of the aggregated result reported by CSP can be verified by user.

4) Guarantee the privacy of the LSD's location (LSDP). Our schemes should ensure any entity except the location-sensitive device itself and the totally trusted user couldnot learn any location information about the legitimate sensing devices.

5) Guarantee the confidentiality of the data (DC). Our schemes should guarantee the data confidentiality against outside attacker (DCO). As the CSP is untrusted, our schemes should also guarantee the data confidentiality against CSP (DCC). In other words, our schemes should ensure the data sensed by location-sensitive devices will not be intercepted by outside attacker and CSP.

6) Guarantee the confidentiality of location strategy (LSC). Our schemes should ensure the confidentiality of user's location strategy. Only the user itself and location-sensitive devices can learn the location strategy.

4. PROPOSED SCHEMES

Starting from this section, we present our LBOA schemes. The scheme $LBOA_{Max}$ which user requests the maximum value of data whose location satisfies user's location strategy. Scheme $LBOA_{Top-k}$ which user requests the largest k values of data whose location satisfies user's location strategy. And, scheme $LBOA_{Sum}$ which user requests the summation value of data whose location satisfies the location strategy.

A) $LBOA_{MAX}$

The overview of $LBOA_{Max}$ is shown in Figure 2. Scheme $LBOA_{Max}$ consists of the following five phases: the initialization phase, the request phase, the collection phase, the aggregation phase and the verification phase. Initialization phase generates parameters which are required later. During the request phase, user formulates location strategy and operation function, then sends request messages to CSP. CSP transmits request messages to LSD and requests LSD to submit the value of sensory data. During the collection phase, location-sensitive devices judge whether the location of data meet user's location strategy or not, and then submit the response to CSP. During the aggregation phase, CSP does aggregation task, and then send sthe aggregated result to user. During the verification phase, user verifies the aggregated result reported by the CSP.

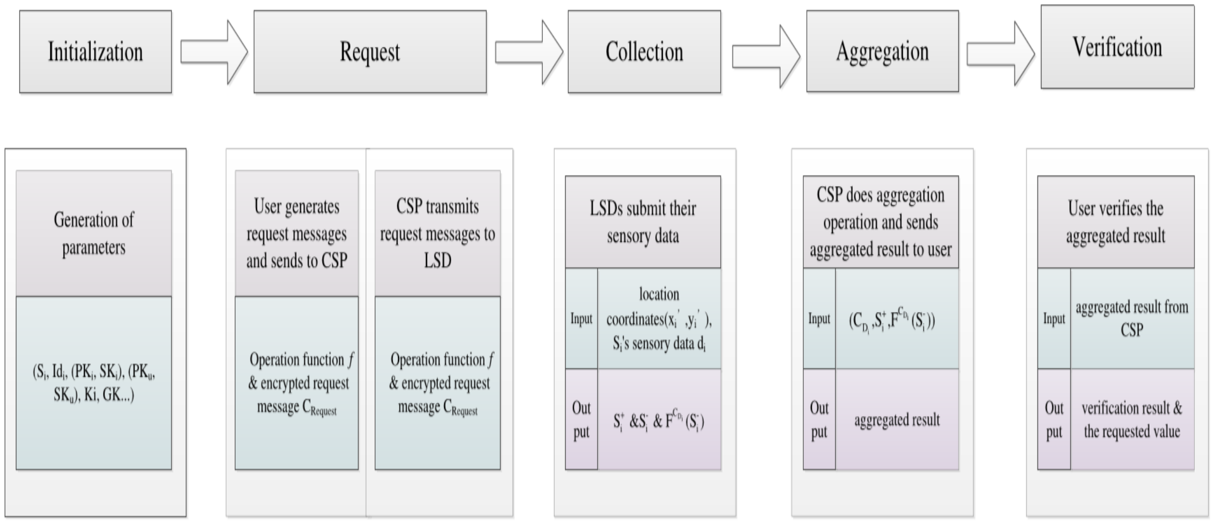

Fig 2. Overview of $LBOA_{Max}$

B) $LBOA_{TOP-K}$

In this section, we do some extension to propose scheme $LBOA_{Top-k}$. User requests to obtain the largest k values of data under location strategy in $LBOA_{Top-k}$ scheme. It is obvious that we can achieve this by executing $LBOA_{Max}$ scheme repeatedly for k times. The first invocation of $LBOA_{Max}$ scheme will return the aggregated result to user. The user could learn the maximum value dm and the location of whoreportingthemaximumvalueofsensorydata.Thenexecutingthesecondinvocationof$LBOA_{Max}$ scheme again after excluding the location-sensitive device Sm. The second invocation will return the second largest value of data. And then, executing the third invocation of $LBOA_{Max}$ scheme again after excluding the location-sensitive device who reports the second largest value of data. In a similar fashion, the user can get top-k values of data whose location satisfy the location strategy after executing $LBOA_{Max}$ scheme repeatedly for k times.

C) $LBOA_{SUM}$

$LBOA_{Sum}$ scheme requests to obtain the summation value of data under user's location strategy. Similar to $LBOA_{Max}$ and $LBOA_{Top-k}$, scheme $LBOA_{Sum}$ also contains of five phases. The initialization phase is completely identical to with an additional initialization step: CSP has a certified public/private key pair that we represent as (PKCSP,SKCSP).

The request phase is identical to except the operation function f is f = Sum, and the user utilizes group key GK to encryption a and the location strategy.

5. RESULTS & DISCUSSION

In this section, we compare our schemes with some related work and the comparison results are shown as below ‘‘√’’means satisfied,‘‘×’’means dissatisfied and‘‘-’’means un involved .LB means location-based, DCO means data confidentiality against outside attacker, DCC means data confidentiality against CSP, LSC means location strategy privacy, LSDP means location-sensitive device privacy, AV means aggregation verifiability.

1) LSD

As shown in Figure 3, we evaluate the computation overhead of LSD in the phase of collection. For $LBOA_{Max}$ and $LBOA_{Top-k}$,wead opt wokinds of different cipher text-space of OPE respectively.

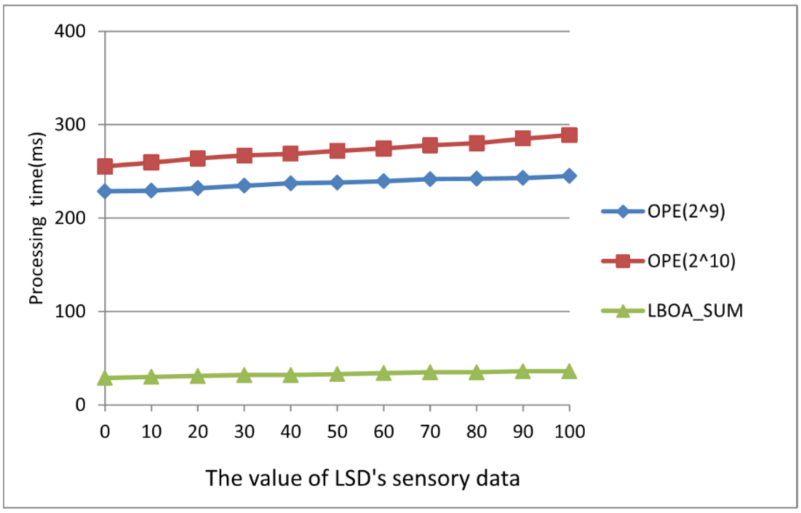

Fig3. Computation overhead of LSD

The computation overhead of LSD in $LBOA_{Top-k}$ is similar to that of $LBOA_{Max}$. In brief, the processing time is between 0.2-0.3 second. It is acceptable for LSD whose calculation and storage power are limited. As for $LBOA_{Sum}$,theprocessingtimeismuchlessthan0.05second. The processing time in $LBOA_{Sum}$ is very short because we do not adopt order-preserving encryption in it. In general, the computation overhead of LSD is practical for LSD who does not have very strong power.

2) CSP

AsshowninFigure4,weevaluatethe computation overhead of CSP in the phase of aggregation in protocol $LBOA_{Max}$. From Figure 4, it is obvious that the number of LSDs satisfying location strategy influence the processing time. The fewer number of LSDs satisfying the location strategy, the higher computation cost of the CSP.

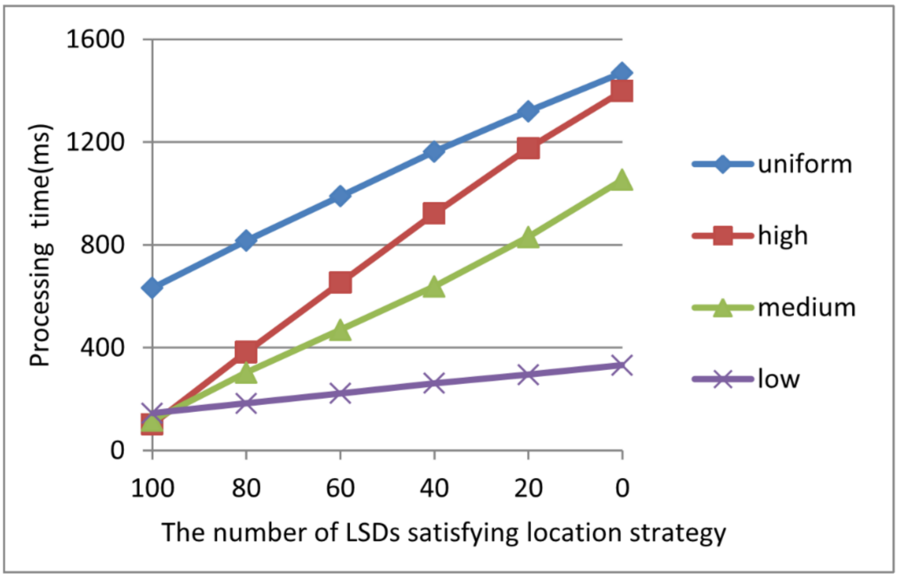

Fig4. Computation overhead of CSP

The processing time is only about 0.1s when all the LSDs' location satisfies user's location strategy, while the processing time is 1.6s when nearly no LSD's location satisfies user's location strategy. The different distribution strategy also affects the computation overhead. It is obvious that the computation overhead is the highest when the values of LSD's sensory data are distributed uniformly, while the computation overhead is the lowest when the values of LSD's sensory data concentrated on low values. The processing time of high distribution is a little longer than that of medium distribution. In general, theprocessingtimeiswithinthescopeof0.1sand1.5s,which is acceptable for CSP in practice.

3) USER

AsshowninFigure5,weevaluatethecomputationoverhead of user in the phase of verification in protocol $LBOA_{Max}$.From Figure 5, the number of LSDs satisfying location strategy has little effect on the computation overhead of user. The distribution strategy of sensory data has much effect on the computation overhead of user.

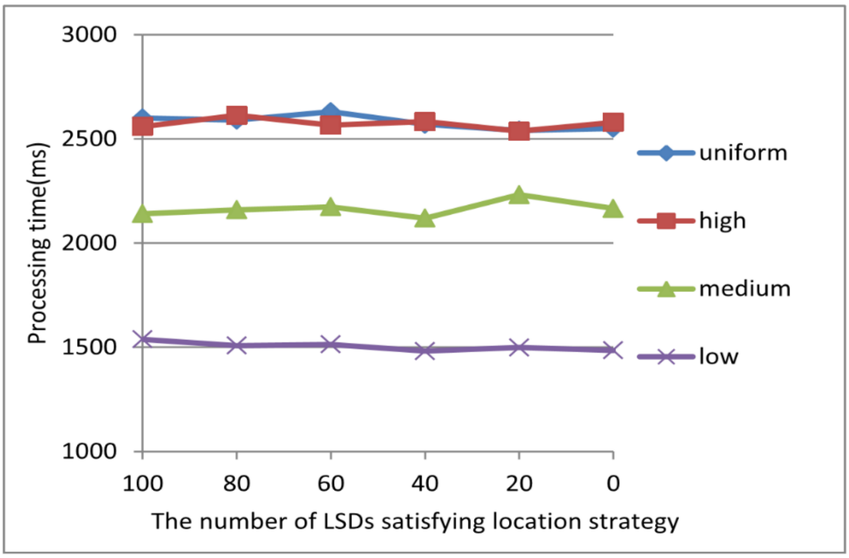

Fig 5. Computation overhead of user

The processing time is about 1.5s, 2.2s, 2.5s and 2.5s when the data distribution strategy is low, medium, high and uniform respectively. The computation over head is the highest when the data values are uniform distribution or high distribution. The computation overhead is the lowest when the data values are low distribution.When the data values are medium distribution, the computation overhead is higher than that of low distribution.

4) Computation Overhead Under Different OPE

As shown in Figure 6, the ciphertext-space of OPE has effect on the computation overhead. We adopt two kinds ofdifferent ciphertext-space of OPE respectively.

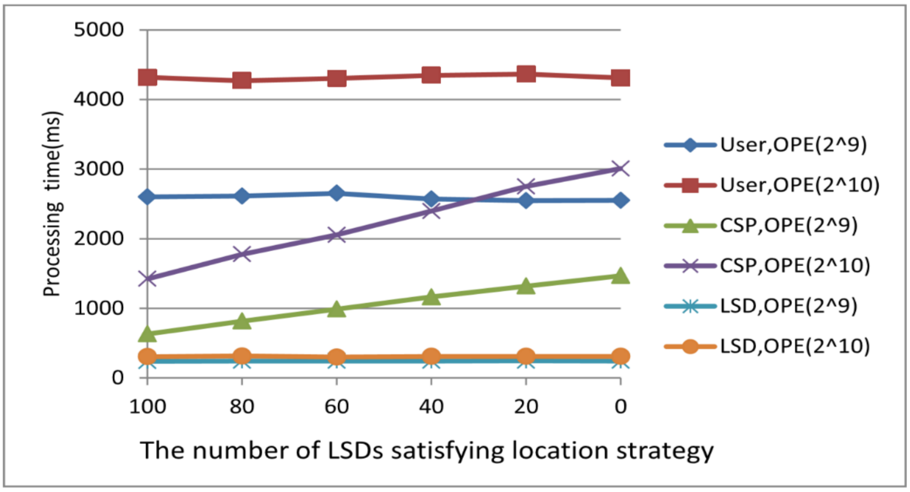

Fig6. Computation overhead under different OPE

ForLSD,thecomputation overhead under OPE (210) is slightly higher than OPE (29). What's more, the computation overhead of LSD is far less than the computation overhead of CSP and user, which is suitable in practice considering that LSD doesnot haves trong capacity for computation.

5) Computation Overhead in LBOA$_{SUM}$

The computation overhead of aggregation in scheme LBOA$_{Sum}$ is shown in Figure 7. The computation overhead of verification in scheme LBOA$_{Sum}$ is shown in Figure 8.

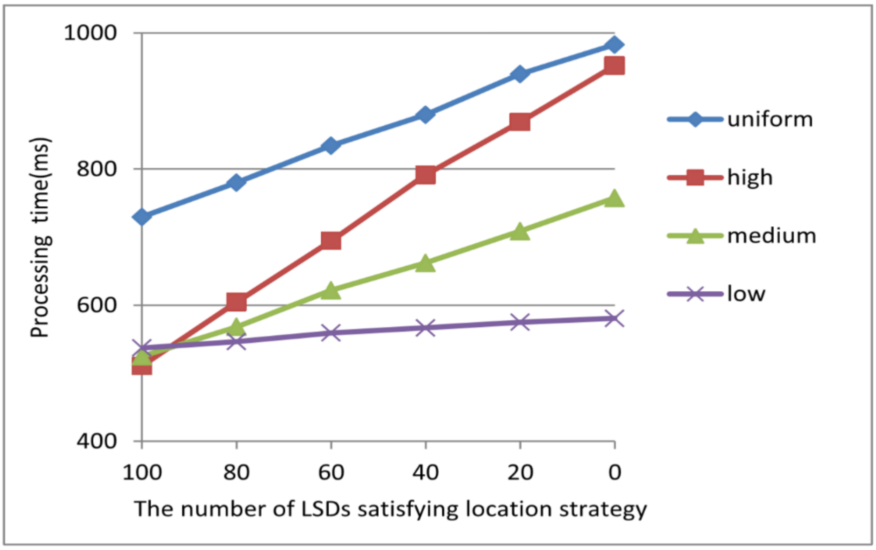

Fig7. Computation overhead of aggregation in LBOA$_{Sum}$

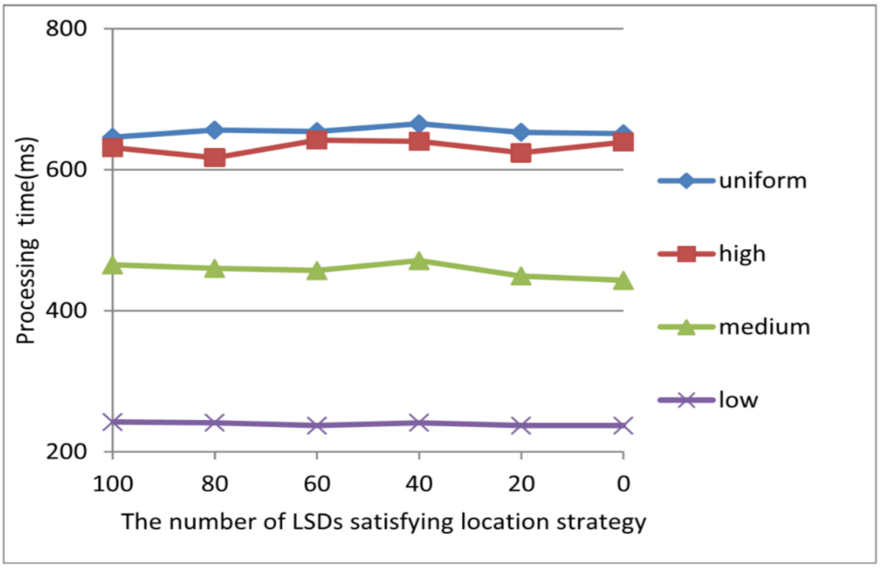

Fig8. Computation overhead of verification in LBOA$_{Sum}$

The computation overhead of LBOA$_{Sum}$ is much lower than that of LBOA$_{Max}$ and LBOA$_{Top-k}$ because Si utilizes public key cryptography rather than order-preserving encryption to encrypt Di in $LBOA_{Sum}$. From Figure 7, it is obvious that the processing time of CSP aggregation is less than 1s. From Figure 8, the processing time of user verification is less than 0.7s, which is acceptable in practice.

6. CONCLUSION

In this study, we proposed three novel schemes that can achieve secure outsourced aggregation based on data's location. We proposed $LBOA_{Max}$ to obtain the Max aggregated data first, and then we proposed $LBOA_{Top-k}$ and $LBOA_{Sum}$ to obtain the Top-k and Sum aggregated data respectively. Different from existing schemes, our schemes could realize secure aggregation based on location and could achieve location privacy protection, data confidentiality protection and location strategy confidentiality protection. Next, we analyze the security of our schemes and the analysis results show that our schemes satisfy all the defined requirements. Finally, the experiment results show that our schemes are practical and feasible in IoT.

REFERENCES

1. X. Li, J. Niu, M. Z. A. Bhuiyan, F. Wu, M. Karuppiah, and S. Kumari, ''ArobustECC-basedprovablesecureauthenticationprotocolwithprivacy preserving for industrial Internet of Things,'' IEEE Trans. Ind. Informat., vol. 14, no. 8, pp. 3599–3609, Aug. 2018.
2. D. Kwon, M. R. Hodkiewicz, J. Fan, T. Shibutani, and M. G. Pecht, ''IoT-based prognostics and systems health management for industrial applications,'' IEEE Access, vol. 4, pp. 3659–3670, 2016.
3. E. Fernandes, J. Jung, and A. Prakash, ''Security analysis of emerging smart home applications,'' in Proc. IEEE Symp. Secur. Privacy (SP), San Jose, CA, USA, May 2016, pp. 636–654.
4. D.LuandT.Liu,''TheapplicationofIoTinmedicalsystem,''inProc.Int. Symp. IT Med. Edu., vol. 1, 2011, pp. 272–275.
5. T. Dimitriou, ''Secure and scalable aggregation in the smart grid,'' in Proc. IEEE Int. Conf. New Technol., Mpbility Secur. (NTMS), Dubai, United Arab Emirates, Mar./Apr. 2014, pp. 1–5.
6. L.HuandD.Evans,''Secureaggregationforwirelessnetworks,''inProc. Appl. Internet Workshops, Orlando, FL, USA, 2003, pp. 384–391.
7. H. Xiong, K.-K. R. Choo, and A. V. Vasilakos, ''Revocable identity-based access control for big data with verifiable outsourced computing,'' IEEE Trans. Big Data, to be published.
8. F. Deng, H. Xiong, Y. Wang, L. Peng, J. Geng, and Z. Qin, ''Ciphertextpolicy attribute-based signcryption with verifiable outsourced designcryption for sharing personal health records,'' IEEE Access, vol. 6, pp. 39473–39486, 2018.

9. G.Xie,G.Zeng,R.Li,andK.Li,‘‘Quantitativefault-toleranceforreliable workflows on heterogeneous IaaS clouds,’’ IEEE Trans. Cloud Comput., to be published. doi: 10.1109/TCC.2017.2780098.
10. Y. Chen, G. Xie, and R. Li, ‘‘Reducing energy consumption with cost budget using available budget pre assignment in heterogeneous cloud computing systems,’’ IEEE Access, vol. 6, pp. 20572–20583, 2018.
11. Viswanth, V. S., Ramanujam, R., and Rajyalakshmi, G.. “Performance study of eco-friendly dielectric in EDM of AISI 2507 super duplex steel using Taguchi-fuzzy TOPSIS approach”. International Journal of Productivity and Quality Management, 29(4), 518-541, 2020.
12. H. Xiong, H. Zhang, and J. Sun, ‘‘Attribute-based privacy-preserving data sharing for dynamic groups in cloud computing,’’ IEEE Syst. J., to be published.
13. J. Zhang, J. Ma, C. Yang, and L. Yang, ‘‘Universally composable secure positioning in the bounded retrieval model,’’ Sci. China Inf. Sci., vol. 58, no. 11, pp. 1–15, 2015.
14. T.Kwon,J.Lee,andJ.Song,‘‘Location-basedpairwisekeypredistribution for wireless sensor networks,’’ IEEE Trans. Wireless Commun., vol. 8, no. 11, pp. 5436–5442, Nov. 2009.
15. B. Li, W. Wang, Q. Yin, H. Li, and R. Yang, ‘‘An energy-efficient geographic routing based on cooperative transmission in wireless sensor networks,’’ Sci. China Inf. Sci., vol. 56, no. 7, pp. 1–10, 2013.
16. Viswanth, V. S., Ramanujam, R., and Rajyalakshmi, G. A review of research scope on sustainable and eco-friendly electrical discharge machining (E-EDM). Materials Today: Proceedings, 5(5), 12525-12533, 2018.
17. A. Boldyreva, N. Chenette, Y. Lee, and A. O’Neill, ‘‘Order-preserving symmetric encryption,’’ in Proc. Annu. Int. Conf. Theory Appl. Cryptograph. Techn., Cologne, Germany: Springer, 2009, pp. 224–241.

Author’s Profile:

Mr. B Sunil Kumar has received his M.Sc Computer Science from SVU PG Center, Kavali affiliated to Sri Venkateswara University in 2002, M.Tech degree in Information Technology from Sathyabama University, Chennai in 2009 and M.Tech in Computer Science and Engineering from SVCET, Chittoor affiliated to JNTU, Anantapur in 2013. He is pursuing Ph.D in CSE at SVU, Uttar Pradesh. He is dedicated to teaching field from the last 14 years. He has guided 26 P.G and 40 U.G students. His research areas included Data Mining. At present he is working as Assistant Professor in Narayana Engineering College, Gudur, Andhra Pradesh, India.

M. Kiran Kumarhas received his B.Sc degree in Computer Science from Krishna Chaitanya Degree College, Nellore affiliated to Vikrama Simhapuri University, Nellore in 2017 and pursuing PG degree in Mater of Computer Applications (MCA) from Narayana Engineering College, Gudur affiliated to JNTU, Ananthapur, AndhraPradesh, India.

