Volume 8, No. 5, May-June 2017
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

Location Based Services Data Compression with Privacy Preserving in WSNs

K. Vijaya Bhaskar
Research Scholar, Dept. of Computer science
SV University, TIRUPATI, AP, India

Dr. R. Seshadri
Professor & Director, Computer Centre
SV University, TIRUPATI, AP, India

Dr. A. Rama Mohan Reddy
Professor & Head, Dept. of CSE
SVU College of Engineering
SV University, TIRUPATI, AP, India

Abstract: In two-layered sensor arrange engineering stockpiling hubs assemble information from close-by sensors and answer questions from the sink of the system. The capacity hubs fill in as a middle of the road level between the sensors and the sink for putting away information and preparing questions. Utilizing homomorphic encryption conspires; a Location-Based Service (LBS) can handle scrambled contributions to recover encoded area related data. The recovered encoded information must be unscrambled by the client who asked for the information. The innovation still confronts two primary difficulties: the experienced handling time and as far as possible forced on the permitted number of operations. In any case, the security of clients' protection accomplished through this innovation makes it alluring for more research and upgrading. Sprout channels speak to a huge information with a little information. In this way, a sensor just needs to send the Bloom channel rather than the hashes to a capacity hub. The quantity of bits expected to speak to the Bloom channel is much littler than that expected to speak to the hashes. For better execution as far as speed and calculations we propose to utilize compacted Bloom channels than plain ones. By utilizing compacted Bloom channels, sensor hubs can diminish the quantity of bits communicates, the false positive rate, or potentially the measure of calculation per query. The cost is the preparing time for pressure and decompression, which can utilize basic number juggling coding, and less memory use at the capacity hubs, that uses the bigger uncompressed type of the Bloom channel. A down to earth usage of the proposed framework approves our claim.

Keywords: Wireless Sensor Networks, Privacy preserving, Bloom filters, Compressed Bloom Filter, Location Based Services, Homomorphic Encryption.

I. INTRODUCTION

A Wireless Sensor Networks (WSN) comprises of spatially conveyed self-governing sensors to screen ecological or physical conditions like weight, sound, temperature et cetera. It has been broadly sent for differed applications, such as setting detecting, building security observing, and seismic tremor expectation et cetera. We consider a two-layered sensor arrange engineering in which stockpiling hubs assemble information from adjacent sensors and answer questions from the sink of the system.

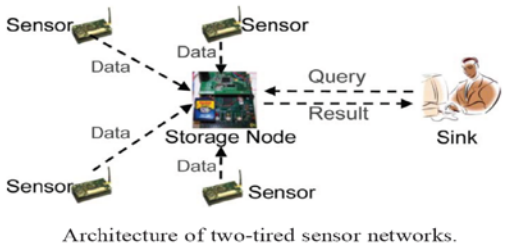


Figure 1: Wireless sensor network architecture

A transitional level between the sensors and the sink fills in as the capacity hub for handling inquiry and the putting away information. Capacity hubs convey three primary advantages to sensor systems [1-3].

a. Sensors spare power by sending every gathered data to their nearest stockpiling hub as opposed to sending them to the sink through long courses.

b. Sensors can be memory-constrained in light of the fact that information are for the most part put away on capacity hubs.

c. Inquiry preparing turns out to be more productive in light of the fact that the sink just speaks with capacity hubs for inquiries. As capacity hubs store information got from sensors and fill in as a vital part to answer questions, they are more helpless against be bargained, particularly in a threatening domain. The capacity hub forces the noteworthy dangers to a sensor arrange.

• The aggressors may get touchy information that has been put away in the capacity hub. • The capacity hub may give back the manufactured information for the inquiry.

• This stockpiling hub may exclude all information things that fulfill the inquiry.

We need to plan a convention that keeps aggressors from picking up data from both sensor-gathered information, sink issued inquiries, and permits the sink to identify traded off capacity hubs when they get into mischief. For Privacy, bargaining a capacity hub ought not permit the aggressor to acquire the delicate data that has been put away in the hub [4-6]. And additionally the inquiries that the capacity hub has gotten, and will get. For Integrity, the sink needs to identify whether an inquiry result from a capacity hub incorporates manufactured information things or does exclude every one of the information that fulfill the question. For comprehending the protection and honesty, there are two key difficulties.

 A capacity hub needs to effectively handle encoded inquiries over encoded information without knowing their genuine qualities.

 A sink needs to confirm that the consequence of an inquiry contains every one of the information things that fulfill the question and does not contain any produced information.

Location based services utilizes a novel strategy to encode both information and inquiries to such an extent that a capacity hub can accurately handle encoded questions over encoded information without knowing their real values to save the trustworthiness. We propose two plans

 One utilizing Merkle hash trees

 another information structure called neighborhood chains.

We propose an answer for adjust Location based services for occasion driven sensor organizes then a sensor submits information to its adjacent stockpiling hub just when a specific occasion happens and the occasion may happen rarely. Our outcomes demonstrate that the power and space reserve funds of Location based services over earlier workmanship develop exponentially with the quantity of measurements. Location based services devours 184.9 circumstances less power for sensors and 76.8 circumstances less power for capacity hubs for three-dimensional information.

II. BACKGROUND WORK

In two-layered sensor organize design stockpiling hubs accumulate information from close-by sensors and answer inquiries from the sink of the system. The capacity hubs fill in as a middle of the road level between the sensors and the sink for putting away information and handling inquiries. Capacity hubs convey three fundamental advantages to sensor systems. To start with, sensors spare power by sending every single gathered dat to their nearest stockpiling hub as opposed to sending them to the sink through long courses [7-9]

- Second, sensors can be memory-restricted on the grounds that information are primarily put away on capacity hubs.
- Third, question preparing turns out to be more proficient in light of the fact that the sink just speaks with capacity hubs for inquiries.

  A few results of capacity hubs, for example, Star Gate and RISE, are industrially accessible proposing their significance. Security challenges. As capacity hubs store information got from sensors and fill in as an essential part to answer inquiries, they are more defenseless against be traded off, particularly in an unfriendly domain. Bargained stockpiling hub forces critical dangers to a sensor organize. For trustworthiness, the sink needs to recognize whether a question result from a capacity hub incorporates manufactured information things or does exclude every one of the information that fulfill the inquiry [10]. There are two key difficulties in settling the protection and honesty safeguarding range question issue.
- First, a capacity hub needs to accurately handle encoded questions over encoded information without knowing their real values.
- Second, a sink needs to check that the aftereffect of a question contains every one of the information things that fulfill the inquiry and does not contain any fashioned information.

Customarily propose to create Location based administrations, a novel security and trustworthiness saving reach inquiry convention for two-layered sensor arranges that keeps assailants from picking up data from both sensor gathered information and sink issued inquiries, which commonly can be demonstrated as range questions, and permits the sink to recognize traded off capacity hubs when they get out of hand [11].

1.The thoughts of Location based administrations are in a general sense not quite the same as the S&L conspire.

2.To save security, Location based administrations utilizes a novel method to encode both information and questions to such an extent that a capacity hub can effectively prepare encoded inquiries over encoded information without knowing their genuine qualities [12].

To protect uprightness, we propose two plans—one utilizing Merkle hash trees and another utilizing another information structure called neighborhood chains—to create respectability check data to such an extent that a sink can utilize this data to confirm whether the aftereffect of a question contains precisely the information things that fulfill the inquiry.

III. PROPOSED APPROACH

Presents an improvement system in view of Bloom channels to lessen the correspondence cost amongst sensors and capacity hubs. This cost can be noteworthy due to two reasons. To begin with, in every accommodation, a sensor needs to change over every range inquiry into two factors, where the two factors are two quantities of w bits, to prefix numbers in the most pessimistic scenario. Second, the sensor applies HMAC to every prefix number, which brings about a 128-piece string in the event that we pick HMAC-MD5 or a 160-piece string in the event that we pick HMAC-SHA1 [13-15]. Lessening correspondence cost for sensors is critical in light of force utilization. Our fundamental thought is to utilize a Bloom channel to speak to vast information with a little information. In this way, a sensor just needs to send the Bloom channel rather than the hashes to a capacity hub. The quantity of bits expected to speak to the Bloom channel is much littler than that expected to speak to the hashes. For better execution as far as speed and calculations we recommend to utilize packed Bloom channels than plain ones. By utilizing packed Bloom channels, sensor hubs can lessen the quantity of bits communicates, the false positive rate, or potentially the measure of calculation per query. The cost is the handling time for pressure and decompression, which can utilize straightforward number juggling coding, and less memory use at the capacity hubs that uses the bigger uncompressed type of the Bloom channel.

IV. PRIVACY PRESERVING APPLICATION DEVELOPMENT

As in the single dimensional protection method, every measurement in multi-dimensional is connected. Sensor si gathers 5 two-dimensional information things (1,11), (3,5), (6,8), (7,1) and (9,4), it will apply the 1-dimensional security safeguarding strategies to the main dimensional qualities {1, 3, 6, 7, 9} and the second dimensional qualities {1, 4, 5, 8, 11}. To protect the respectability of multi-

dimensional information we assemble a multi-dimensional neighborhood chain. The dashed bolts represent the chain along the Y measurement and strong bolts delineate the chain along the X measurement [16].

We have accepted that at every schedule opening a sensor sends to a capacity hub the information that it gathered at that availability. This presumption does not hold for occasion driven systems that a sensor just reports information to a capacity hub when a specific occasion happens. The sink can't confirm whether a sensor gathered information at a schedule vacancy when on the off chance that we straightforwardly apply our answer. We address the above test by sensors detailing their sit without moving period to capacity hub every time when they submit information after a sit without moving period or when the sit out of gear period is longer than an edge. Thus, stockpiling hubs can utilize such sit out of gear period announced by sensors to demonstrate to the sink that a sensor did not present any information whenever opening in that sit out of gear period. Sensors: A sit still period for a sensor is a schedule opening interim [t1,t2] that demonstrates that the sensor has no information to submit from t1 and t2. Let be the edge of a sensor being inactive without answering to a capacity hub. Capacity Nodes: When a capacity hub gets an inquiry from the sink then first it checks climate si has submitted information at availability. Sink: Changes on the sink side are negligible.

Table 1: Complexity analysis of the sensor networks with privacy preserving applications.

	Computation	Communication	Space
Sensor	O(*zn*) hash O(*n*) encryption	O(*zn*)	–
Storage node	*O(z)* hash	*O(zn)*	*O(zn)*
Sink	*O(z)* hash	*O(z)*	--

A secured two-layered sensor organize bargaining a capacity hub does not permit the aggressor to get the estimations of sensor-gathered information and sink issued inquiries in the Location based administrations. A capacity hub just gets encoded information things and the protected hash estimations of prefixes changed over from the information things just in the accommodation on the convention. It is computationally infeasible to register the genuine estimations of sensor gathered information, without knowing the keys utilized the relating prefixes in the encryption and secure hashing. The key utilized as a part of the protected hashing is without knowing the computationally infeasible to process the genuine estimations of sink issued inquiries. The aftereffect of inquiry can be identified by the sink, which contains every one of the information things that fulfill the question and whether it contains fashioned information [17].

V. EXPERIMENTAL RESULTS

In this segment we concentrate the execution of our proposed framework. We demonstrate the information stream of our ace postured framework. A client can auto-find himself/herself (the locale where he has a place and his position) utilizing PDA abilities. At that point, the client's product en-graves both his facilitate and the sort of administration he/she is focusing on, and sends them to the server. The server retrieves the asked for targets relying upon the encoded data. From that point, it sends these encoded focuses to the customer to be unscrambled and seen by the client.

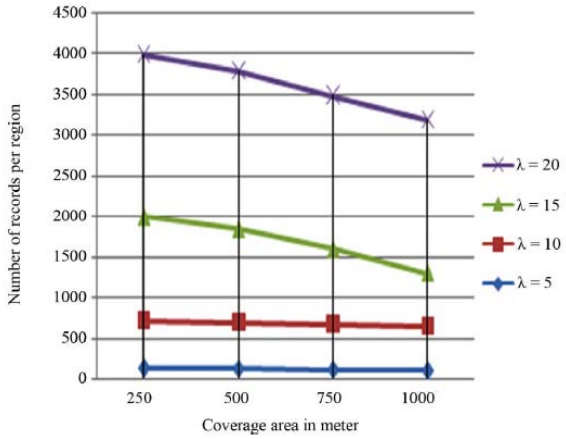


Figure 2: Number of compressed data values in wireless sensor networks with data reliability.

As shown in above figure proposed approach gives efficient data communication in wireless sensor network communication with reliable privacy security issues in location based services.

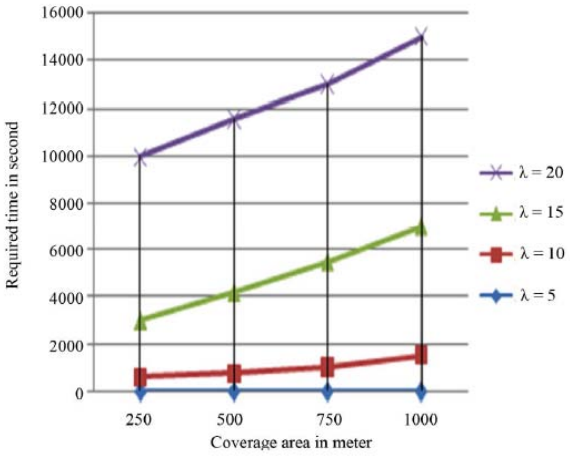
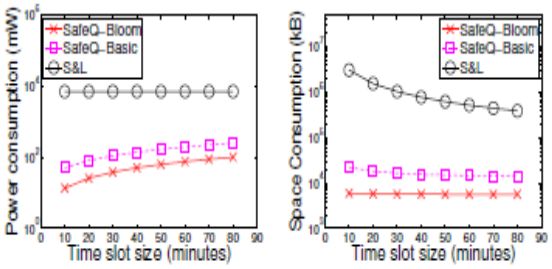


Figure 3: Processing time in data vigilance in wireless sensor networks with respect to compressed data.

Our framework has a confinement as far as the quantity of records it can bolster. As the quantity of the put away tar-gets develops, the framework needs to lead a critical number of math operations. We may even achieve the maximum furthest reaches of the commotion esteem before separating every one of the objectives, and a fruitful decoding won't be guaranteed. Figure 3 shows processing of node utilization in wireless sensor networks. We can beat this issue by utilizing substantial values of security parameter λ. Our experimental results shows the Location based services-Bloom consumes 184.9 times less power for sensors and 182.4 times less space for storage nodes. We implemented both Location based services and the state-of-the-art on a large real data set. For 2-dimensional data, Location based services Bloom consumes 10.3 times less power for sensors and 10.2 times

less space for storage nodes. As shown in the fig.6 the average power and space consumption for 3-dimensional.



(a) Sensor: power consumption (b) Storage node: space consumption

Figure 4: Ave. power and space consumption for 3-dimensional data.

The three-dimensional shows the Location based services-NC+ consumes 182.4 times less space and Location based services-MHT+ consumes 169.1 times less space. As shown in the fig.2 the average space consumption of storage nodes for each data item versus the number of dimensions of the data item.

VI. CONCLUSION

Presents an enhancement method in view of Bloom channels to diminish the correspondence cost amongst sensors and capacity hubs. Our fundamental thought is to utilize a Bloom channel to speak to a huge information with a little information. In this manner, a sensor just needs to send the Bloom channel rather than the hashes to a capacity hub. The quantity of bits expected to speak to the Bloom channel is much littler than that expected to speak to the hashes. For better execution as far as speed and calculations, we recommend utilizing packed Bloom channels than plain ones. By utilizing compacted Bloom channels, sensor hubs can decrease the quantity of bits communicates, the false positive rate, or potentially the measure of calculation per query. The cost is the handling time for pressure and decompression, which can utilize straightforward math coding, and less memory use at the capacity hubs, that uses the bigger uncompressed type of the Bloom channel.

VII. REFERENCES

[1] "Privacy- and Integrity-Preserving Range Queries in Sensor Networks", by Fei Chen and Alex X. Liu, IEEE/ACM TRANSACTIONS ON NETWORKING,2012.

[2] F. Chen and A. X. Liu, "Location based services: Secure and efficient query processing in sensor networks," in Proc. IEEE INFOCOM, 2010, pp. 1–9.

[3] B. Sheng and Q. Li, "Verifiable privacypreserving range query in two-tiered sensor networks," in Proc. IEEE INFOCOM, 2008, pp. 46–50.

[4] Xbow, "Stargate gateway (spb400)," 2011 [Online]. Available: http:// www.xbow.com.

[5] M. Narasimha and G. Tsudik, "Authentication of outsourced databases using signature aggregation and chaining," in Proc. DASFAA, 2006, pp. 420–436.

[6] W. Cheng, H. Pang, and K.-L. Tan, "Authenticating multi-dimensional query results in data publishing," in Proc. DBSec, 2006, pp. 60–73.

[7] H.Chen, X.Man,W.Hsu, N. Li, and Q.Wang, "Access control friendly query verification for outsourced data publishing," in Proc. ESORICS, 2008, pp. 177–191.

[8] R. Merkle, "Protocols for public key cryptosystems," in Proc. IEEE S&P, 1980, pp. 122–134.

[9] E.-J. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing remote untrusted storage," in Proc. NDSS, 2003, pp. 131–145.

[10] Youssef Gahi, Mouhcine Guennoun, Zouhair Guennoun, Khalil El-Khatib, " Privacy Preserving Scheme for Location-Based Services", Journal of Information Security, 2012, 3, 105-112.

[11] G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi and K.-L. Tan, "Private Queries in Location-Based Services: Anonymizers Are Not Necessary," Proceedings of the SIGMOD 08, Vancouver, 9-12 June 2008, pp. 121-132.

[12] C. Gentry and Z. Ramzan, "Single-Database Private Information Retrieval with Constant Communication Ra- te," Proceedings of the 32nd International Colloquium on Automata, Languages and Programming, Lisboa, 11-15 July 2005, pp. 803-815.

[13] D. Rebollo-Monedero and J. Forne, "Optimized Query Forgery for Private Information Retrieval," IEEE Transactions on Information Theory, Vol. 56, No. 9, 2010, pp. 4631-4642. doi:10.1109/TIT.2010.2054471

[14] Y. Gahi , M. Guennoun and K. El-khatib, "A Secure Database System Using Homomorphic Encryption Schemes," Proceedings of the 3rd International Conference on Advances in Databases, Knowledge, and Data Applications, St. Maarten, 23-28 January 2011, pp. 54-58.

[15] C. Y. Chow, M. F. Mokbel and X. Liu, "A Peer-to-Peer Spatial Cloaking Algorithm for Anonymous Location- Based Services," Proceedings of the 14th Annual ACM International Symposium on Advances in Geographic Information Systems, Arlington, 10-11 November 2006, pp. 171-178. doi:10.1145/183471.1183500

[16] B. Gedik and L. Liu, "Location Privacy in Mobile Sys-tems a Personalized Anonymization Model," Proceedings of the 25th International Conference on Distributed Com- puting System of the IEEE ICDCS, Columbus, 10 June 2005, pp. 620-629. doi:10.1109/ICDCS.2005.48.

[17] M. F. Mokbel, C. Y. Chow and W. G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy," Proceedings of the VLDB 2006, Seoul, 12-15 September 2006, pp. 763-774.