ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

Productive and Privacy-Aware Data Aggregation in Mobile Sensing

[1] Vinaysagar Anchuri
[1] Assistant Professor, Department of Computer Science Engineering,
Guru Nanak Institute of Technology, Ibrahimpatnam, Ranga Reddy, Telangana, India

Abstract - **Cell phones particularly advanced mobile phones are getting increasingly significance in everyday life. A greater amount of these cell phones are currently encouraged with number of uses that are utilizing sensors. With the assistance of extensive no. of individual members, total which is registered from information is truly valuable and predicts the measurements of result. Total ensures more protection of the information from singular members. This paper gives an answer for protecting the individual members security by utilizing total capacity like Sum, Min. Count of Sum accumulation is managed without discharging the member's data. Min accumulation is computed utilizing Sum collection. Min total is only least estimation of information. In this paper, a multi-bounce arrange is considered where, there is a principle aggregator at the largest amount and portable hubs are considered at most reduced level and in the middle of hub sink is utilized at center level. This framework manages dynamic leaves and participates in versatile detecting utilizing the timestamp of the members.**

Keywords — Encryption, Multi-hop network, Mobile Sensing, Data Aggregator, Privacy

I. INTRODUCTION

The Wireless Mobile remote sensor system can be just characterized as WSN with versatile as sensor hubs. These hubs comprise of a radio transreceiver and a microcontroller fueled by a battery. The topology utilized for these systems isn't chosen. Along these lines, steering winds up plainly difficult occupation. Information Aggregation is only accumulation of information from various assets or hubs and giving yield as asummary.The collection insights are typically registered intermittently to investigate its example. The source data for information aggregators may begin from open records anddatabases, the data is bundled into total reports and after that may sold to various organizations. These reports can be utilized as a part of individual verifications and to settle on a few choices. The majority of the works in this consider the aggregator is trusted. Be that as it may, this isn't the situation each time. The test is to secure information when the aggregator is untrusted. Huge numbers of the current works [2][3],consider the time arrangement information and untrusted aggregator. In this, with the end goal of assurance of information, another encryption plot is presented. In these plans, aggregator decodes just the entirety of every one of clients' information rather than singular client's information. In this paper, we propose a convention to get whole total in multichip organize and considering the untrusted Aggregator. In PC organizing, a bounce speaks to one bit of the way amongst source and goal. When imparting over the web, information goes through various middle of the road gadgets like switches as opposed to

streaming straightforwardly finished a solitary wire .Each such gadget makes information bounce between one pointto point organize associations. In this paper we consider a multihopnetwork where three levels are kept up. The most reduced level comprises of portable hubs and in the center level there are hub sink and at largest amount there is principle aggregator. Clients may join and leave in versatile detecting systems. So in the propose conspire dynamic leaves and joins are kept up with the assistance of parameters like thickness, separation and time. With the assistance of total aggregation.min accumulation is ascertained. In next segment II we ar introducing the writing study over various techniques displayed.

II. RELATED WORK

In the literature survey section we are going to discuss about recent methods regarding: QinghuaLi, GuohongCao, ThomasF.LaPorta [1] introduced the scheme that is based on the increasing capabilities of smart phones This scheme provides privacy to each user by obtaining Sum aggregate and Min aggregate. This

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

scheme uses HMAC based key management technique to perform efficiently. This scheme uses redundancy in security to reduce cost of joins and leaves. The scheme deals with limited number of users. VibourRastogi and SumanNath [2] propose the first differentially private aggregation algorithms for distributed time series data with untrusted server called PASTE. PASTE focuses on data mining applications which consist of an untrusted aggregator that is to run aggregate queries on the data. PASTE uses two algorithms that are Fourier Perturbation Algorithm (FPA) and Distributed Laplace Perturbation Algorithm (DLPA).PASTE proposes a pair of algorithms that answer queries on time-series data. FPA is used to answer long query sequences in a parallel way and DLPA implements Laplace noise addition in distributed way. In this scheme, for communication between users and aggregator, a extra round is required which makes the scheme costly. Elaine Shi,T-H HubretChan,Rieffel[3] introduces a system that maintains the privacy of each participant and considers the untrusted aggregator. In this construction, a group of participants periodically uploads the data and aggregator computes the sum of all data. The two important aspects that are focused in this construction is data randomization procedure and encryption at each participant or user with separate key. This paper describes Private Stream Aggregation (PSA) that consists of encrypted data of use that is uploaded to aggregator. This scheme may not work for large systems or we can say multilevel systems. Yang, Zhong and Wright [4] proposes a cryptographic approach that is able to maintain many customers and their settings and provides them privacy. In this frequencies of values are computed from the customer's data. It do not require any communication between customers .Each customer needs to send a single flow .This scheme becomes quite expensive if rekeying is required and hence this scheme may not be work worthily for time series data. Shi, Y.Zhang, Liu and R.Zhang [5] proposes data aggregation scheme that uses data slicing and mixing techniques. This scheme cannot be used for time-series data. The overall scheme takes long delays as it takes number of rounds between users and aggregator for communication. The aggregation functions can be applied to this scheme but it is quite costly.

III. PROBLEM STATEMENT

The System introduces sum aggregation of time-series data in the presence of an untrusted aggregator. Based on sum aggregate, a protocol for Min aggregate is proposed. Also, the scheme deals with dynamic leaves and joins

IV. PRELIMINARIES

A. A Straw-man Construction

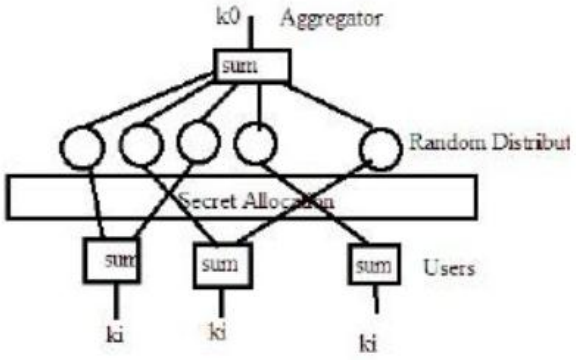

Fig. 1. Straw man Construction

Consider that there are nc random numbers. The aggregator calculates the sum of all these numbers and this is used as decryption key. Consider k0 as decryption key.nc Random numbers are divided into n users and each user is assigned with unique subset of nc.Each user calculates sum of all numbers assigned to it and set it as encryption key. Consider ki as encryption key of user i. Let S denote the set of secrets and Si denotes ith subset. Lets consider that s1,s2,snc be the different secrets.
Encryption Key Generation
ki =Σh(fs(t))modM
Decryption key Generation
k0 =Σh(fs(t))modM

V. PROPOSED SYSTEM FRAMEWORK AND DESIGN

A. ARCHITECTURE

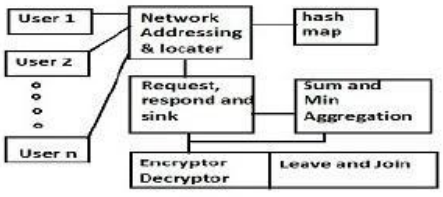

Fig.2System Architecture

B. Network Model

In the network model, the nodes are placed in the most bottom of the network model. The node sink is used to manage the nodes. The node sink behaves like a cluster head of the mobile nodes. At the highest level, there is main aggregator where the actual sum and min

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

aggregation is done. For communication between two nodes, both of them need to communicate through main aggregator and respective node sinks. Dynamically the leaves and joins are maintained for this network using factors like distance of each node.

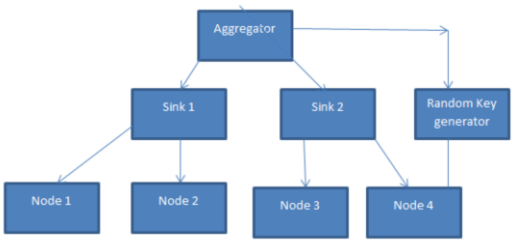

Fig 3: Network Model

The proposed algorithm for data aggregation and session key generation and each detailing of techniques are described in section 3.C.

C. Algorithms

Algorithm 1: For Network Model

Level 1
If (S is Secure)
then, combine all sensor data
from its own region
End if
Level 2
If(S€Sn)
then, check present sessionId
if(sessionId not present)
then create new data set
End if
Level 3
If(not)
Check that data present in TDS
or not
Check if same sessionId
Else
Forward data to nearest Base
station
Entry to TDS
Session encrypt data
Add sessionId
Apply signature on it

Algorithm 2: At Main Aggregator

1. Create a server Socket.
2. Generate a PVSS engine passing the number of secrets, the threshold and the number of bits to be used.
3. Generate n secret keys (one for each party)
4. Generate n public keys using the corresponding secret keys
5. Generate the encrypted shares and their proof
6. Each party verify the received decrypted share
7. Each party extract its share with the help of min .
8. Combine the first T shares to obtain the secret back i.e the sum is caluculated.
9. Depending upon the time stamp decided prior ,the node is allowed to join or not is decided.

D. Mathematical Model

We can describe the system mathematically. Let A be the overall system. So, A can be described as A is a set of input, output, process. So, diagrammatically the system can be described as:

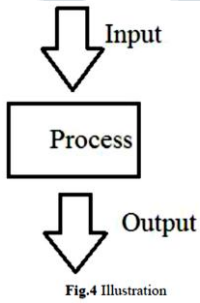

Fig.4 Illustration

Input is file containing data from source Output is file containing data at destination more securely Process:
1.Sum aggregation
S=S.multiply(Sh[x[i].modPow(Sh[x[i]].modPow(lambda, q)).mod q
Where
S is secret and Sh is Share generated.
2.Min aggregation
M=min(S)
3.Dynamic Leaves and Joins
t = time for communication
if t <threshold value`
then allow a node to join
if t >threshold value
then allow a node to leave.

VI. PRACTICAL RESULTS AND ENVIRONMENT

In this section we are presenting practical environment, dataset used, and metrics computed.

A. Software Used

Software Configuration

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 4, Issue 2, February 2017

- Operating System: Windows 7
- Programming Language: Java

B. Results

Input
1. Request from sender node
2. File from one node.

Output
File is received at destination node with more security.

Results

	Security	No. of nodes manage	Time to receive packets	Dependencies
Previous System	Less	Less	Less	Aggregator
Proposed System	More	More	Moderate	On main aggregator and sink node

Table 1: Comparision of previous and proposed system

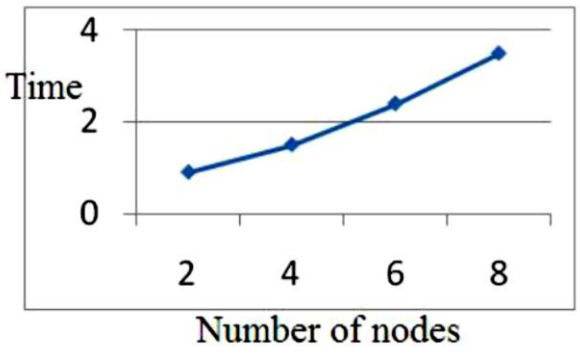

Fig 5: Graph of proposed system

The comparison of previous and proposed system is given in Table 1.The factors like security, Number of nodes the system can manage; dependencies etc are used to compare the proposed system with previous systems. Previously, a single level containing different nodes is managed. So, there is a restriction on number of nodes the system can manage. As this is multichip system and we are maintain three levels, the more number of nodes can be managed by the system. There can be slight difference in receiving packet. At each level encryption and decryption is done. So, it may take some more time but it provides more security as compared to previous one. The graph is plotted against number of nodes and time required. \As the number of nodes increased, the time will increase.

VII. CONCLUSION

This paper gives every client its own particular protection with entirety conglomeration of individual clients information. The convention utilizes MAC based key administration method to give effective accumulation. This convention will deal with a greater number of clients than existing framework. In view of the Sum total convention, Min total is computed. To manage dynamic leaves and joins the components like thickness, remove is considered. The fundamental point of this task is to present a protected Multilink Time Stamp plot. To achieve this target, the safe and ideally effective Straw-man sort amassed Key variation was reached out to a multiparty setting to yield a MultisinkTime Stamp plot, which gives an ensured traceability property. The proposed Multilink Time Stamp conspire was appeared to fulfill the majority of the predetermined security necessities and satisfies the more grounded break-safe property. The MultisinkTime Stamp collected Key plan consequently stays secure, regardless of whether the limit cryptosystem has been broken, i.e., the gathering mystery or individual mystery shares are known or controlled by a foe. The productivity investigation demonstrated that the proposed MultisinkTime Stamp plot beats other existing plans and is ideal as far as exponentiations concerning edge collected Key check and close ideal for individual accumulated Key confirmation, while giving break protection.

REFERENCES

[1] QinghuaLi,GuohongCao,Thomas F. La Porta,Efficient and Privacy-Aware Data Aggregation in Mobile Sensing, IEEE transaction on Dependable and Secure Computing, Vol. 11,No. 2,March/April 2014

[2] V. Rastogi and S. Nath, Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption, Proc. ACM SIGMOD Intl Conf. Management of Data, 2010.

[3] E. Shi, T.-H.H. Chan, E. Rieffel, R. Chow, and D. Song, Privacy Preserving Aggregation of Time-Series Data, Proc. Network and Distributed System Security Symp. (NDSS 11), 2011.

[4] J. Shi, R. Zhang, Y. Liu, and Y. Zhang, Prisense: Privacy Preserving Data Aggregation in People-Centric Urban Sensing Systems, Proc. IEEE INFOCOM, pp. 758-766, 2010.

[5] Z. Yang, S. Zhong, and R.N. Wright, Privacy-Preserving Classification of Customer Data without Loss of Accuracy, Proc. Fifth SIAM Intl Conf.Data Mining (SDM 05), pp. 21-23, 2005.

[6] M. Jawurek and F. Kerschbaum, Fault-Tolerant Privacy- Preserving Statistics, Proc. 12th Privacy Enhancing Technologies Symp.(PETS 12), 2012.

[7] M. Shao, Y. Yang, S. Zhu, and G. Cao, Towards Statistically Strong Source Anonymity for Sensor Networks, Proc. IEEE INFOCOM, 2008.

[8] C. Castelluccia, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, Proc. Second Ann. Intl Conf. Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous 05), pp. 109-117, 2005.

[9] M. Bellare, New Proofs for NMAC and HMAC: Security without Collision-Resistance, Proc. 26th Ann. Intl Conf. Advances in Cryptology (CRYPTO 06), pp. 602-619, 2006.

[10] Q. Li and G. Cao, Providing Privacy-Aware Incentives for Mobile Sensing, Proc. IEEE PerCom, 2013.