

Data Aggregation using Multi Hop Technique with Security

Chetna Upasani¹, Prof. Tejashree Gaikwad², Prof. Rama Gaikwad³, Prof. Pranali Mahadik⁴

¹ Department of Computer Engineering RCPIT, Shirpur, India

^{2,3,4} Department of Computer Engineering, ABMSP's APCOER, Pune, India

chetnakulkarni1@gmail.com, tejashree.gaikwad@abmspcoerpune.org, rama.coer@gmail.com,
pranali72@gmail.com

Article Info

Page Number: 09-15

Publication Issue:

Vol. 67 No. 1 (2018)

Abstract

In the coming future of Digital Media Smart Mobile Devices are getting more and more importance. The use of these smart devices in day to today life of human being have been increased and it becomes very easy to share information through these devices to others. These mobile devices are now facilitated with number of applications that are using sensors such as camera, microphone, GPS, accelerometer, ambient light sensor, gyroscope and so on. But the data shared by an individual have to be protected. And to maintain the privacy of the important data, the shared data have to be protected. With the help of large numbers of individual participants, aggregation which is computed from data is really useful and helps to predict the statistics of Result. Aggregation guarantees more privacy of the data from individual participants. This paper provides a solution for preserving the individual participants privacy by using aggregate function like Sum, Min. Calculation of Sum aggregation is done without releasing the participant's information. Min aggregation is calculated using Sum aggregation. Min aggregation is nothing but minimum value of data. In this paper, a multi-hop network is considered where, there is a main aggregator at the highest level and mobile nodes are considered at lowest level and in between node sink are used at middle level. This system deals with dynamic leaves and joins in mobile sensing using the timestamp of the participants.

Article History

Article Received: 15 October 2018

Revised: 24 November 2018

Accepted: 18 December 2018

Keywords: - Fire detection, image processing, Real time detection, CCTV (Closed Circuit TV)

Introduction

The Wireless Mobile wireless sensor network can be simply defined as WSN with mobile as sensor nodes. These nodes consist of a radio Trans receiver and a microcontroller powered by battery. The topology used for this network is not decided. So, routing becomes challenging job. Data Aggregation is nothing but collection of data from different resources or nodes and giving output as a summary. The aggregation statistics are normally computed periodically to analyses its pattern. The source information for data aggregators may originate from public records and databases, the information is packaged into aggregate report and then may sold to different agencies. These reports can be used in background checks and to make some decisions. Most of the works in this consider that the aggregator is trusted. But this is not the

case each time. The challenge is to protect data when the aggregator is untrusted. Many of the recent works[2][3], consider the time series data and untrusted aggregator. In this, for the purpose of protection of data, a new encryption scheme is introduced. In this schemes, aggregator decrypts only the sum of all users data instead of individual users data pick before observe the equivalent keyword search trapdoors. It seems an suitable security concept, particularly if the keyword space has no high min-entropy.

In this paper, we propose a protocol to get sum aggregate in multi-hop network and considering the untrusted aggregator. In computer networking, a hop represents one portion of the path between source and destination. When Communicating over the internet, data passes through a number of intermediate devices like routers rather than flowing directly over a single wire. Each such system reasons facts to hop between one factor to factor community connections. In this paper we think about a multihop community the place three degrees are maintained. The lowest stage consists of cellular nodes and in the center stage there are node sink and at best stage there is major aggregator. Users may additionally be a part of and go away in cell sensing networks. So in the suggest scheme dynamic leaves and joins are maintained with the assist of parameters like density, distance and time. With the assist of sum aggregation. min aggregation is calculated.

1.0 Literature Survey

propose a construction that allows a group of participants to periodically upload encrypted values to a data aggregator, such that the aggregator is able to compute the sum of all participants' values in every time period, but is unable to learn anything else. We achieve strong privacy guarantees using two main techniques. First, we show how to utilize applied cryptographic techniques to We propose the first differentially private aggregation algorithm for distributed time-series data that offers good practical utility without any trusted server [2]. This addresses two important challenges in participatory data-mining applications where (i) individual users wish to publish temporally correlated time-series data (such as location traces, web history, personal health data), and (ii) an untrusted third-party aggregator wishes to run aggregate queries on the data. To ensure differential privacy for time-series data despite the presence of temporal correlation, we propose the Fourier Perturbation Algorithm (FPA). Standard differential privacy techniques perform poorly for time-series data. To answer n queries, such techniques can result in a noise of $\Theta(n)$ to each query answer, making the answers practically useless if n is large. Our FPA algorithm perturbs the Discrete Fourier Transform of the query answers. For answering n queries, FPA improves the expected error from $\Theta(n)$ to roughly $\Theta(k)$ where k is the number of Fourier coefficients that can (approximately) reconstruct all the n query answers. Our experiments show that $k \ll n$ for many real-life data-sets resulting in a huge error-improvement for FPA. [2] To deal with the absence of a trusted central server, we propose the Distributed Laplace Perturbation Algorithm (DLPA) to add noise in a distributed way in order to guarantee differential privacy. To the best of our knowledge, DLPA is the first distributed differentially private algorithm that can scale with a large number of users: DLPA outperforms the only other distributed solution for differential privacy proposed so far, by reducing the computational load per user from $O(U)$ to $O(1)$ where U is the number of users.[2]

We consider how an untrusted data aggregator can learn desired statistics over multiple participants' data, without compromising each individual's privacy. [3] We allow the aggregator to decrypt the sum from multiple ciphertexts encrypted under different user keys. Second, we describe a distributed data randomization procedure that guarantees the differential privacy of the outcome statistic, even when a subset of participants might be compromised.

We consider applications where an untrusted aggregator would like to collect privacy sensitive data from users, and compute aggregate statistics periodically. For example, imagine a smart grid operator who wishes to aggregate the total power consumption of a neighborhood every ten minutes; or a market researcher who wishes to track the fraction of population watching ESPN on an hourly basis. We design novel mechanisms that allow an aggregator to accurately estimate such statistics, while offering provable guarantees of user privacy against the untrusted aggregator. Our constructions are resilient to user failure and compromise, and can efficiently support dynamic joins and leaves. Our constructions also exemplify the clear advantage of combining applied cryptography and differential privacy techniques.

Several public key cryptosystems with additional homomorphic properties have been proposed so far. They allow performing computation with encrypted data without the knowledge of any secret information. In many applications, the ability to perform decryption, i.e. the knowledge of the secret key, gives a huge power. [6] A classical way to reduce the trust in such a secret owner, and consequently to increase the security, is to share the secret between many entities in such a way that cooperation between them is necessary to decrypt. In this paper, we propose a distributed version of the Paillier cryptosystem presented at Eurocrypt '99. This shared scheme can for example be used in an electronic voting scheme or in a lottery where a random number related to the winning ticket has to be jointly chosen by all participants.

2.0 Existing Method

- Sensor data aggregation assumes a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Several recent works consider the aggregation of time-series data in the presence of an untrusted aggregator. To protect user privacy, they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else.
- Use threshold Paillier cryptosystem to build such an encryption scheme. To decrypt the sum, their scheme needs an extra round of interaction between the aggregator and all users in every aggregation period, which means high communication cost and long delay. Moreover, it requires all users to be online until decryption is completed, which may not be practical in many mobile sensing scenarios due to user mobility and the heterogeneity of user connectivity.

3.0 Proposed Method

Flame detectors are generally only used in high hazard areas such as fuel loading platforms, industrial process areas, hyperbaric chambers, high ceiling areas, and any other areas with atmospheres in which explosions or very rapid fires may occur. Flame detectors are "line of sight" devices as they must be able to see the fire, and they are subject to being blocked by objects placed in front of them. However, the infrared type of flame detector has some

capability for detecting radiation reflected from walls. In this paper we propose a method able to detect fires by analyzing the videos acquired by surveillance cameras. Two main novelties have been introduced: first, complementary information, respectively based on colour, shape variation and motion analysis, are combined by a multi expert system. The main advantage deriving from this approach lies in the fact that the overall performance of the system significantly increases with a relatively small effort made by designer. Second, a novel descriptor based on a bag-of-words approach has been proposed for representing motion.

To develop a robust fire detection system, we need to understand the nature of fire. When the fire temperature is low range changes from red to yellow and when the fire temperature is high range changes to white. The shape of the flame also changes rapidly. Thus, the fire region exhibits a structure of nested rings of colour s changing from white at the core to yellow, orange and red. [2] Depend on this knowledge; the proposed colour edge detection algorithm is composed of the following four components: At first, the image is smoothed by median filter to suppress unwanted noise in image. Secondly, maximum directional differences of sum of gray values i.e. Red+ Green+ Blue are calculated. In the third step, image is threshold and finally the detected edges are thinned to get the proper edge map. Lastly, after the edge is mapped fire is detected and it send alert to fire brigade.

Disadvantages Of Existing System:

- Cannot protect user privacy against untrusted aggregators.
- Existing works do not consider the Min of time-series data.

4.0 system architecture

In the network model, the nodes are placed in the most bottom of the network model. The node sink issued 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 aggregation is done. For communication between two nodes, both of them need to communicate through main aggregator and respective node sinks.

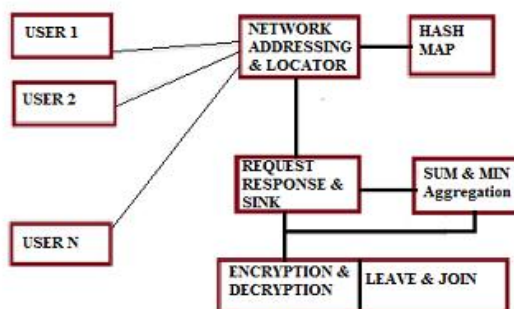


Fig. 1: System Architecture.

Modules:

- System Model Module
- Encryption Scheme Module
- Key Generation Module
- Aggregation Protocol Module

5.0 Modules Description:

System Model Module

In this module first we develop our system model, with mobile users. An aggregator wishes to get the aggregate statistics of n mobile users periodically, for example, in every hour. The time periods are numbered as 1, 2, 3. . . and so on. In every time period, each user i encrypts her data x_i with key k_i and sends the derived ciphertext to the aggregator. From the cipher texts, the aggregator decrypts the needed aggregate statistics using her aggregator capability k_0 . In each time period, a mobile user sends her encrypted data to the aggregator via WiFi, 3G or other available access networks. No peer-to-peer communication is required among mobile users, since such communication is nontrivial in mobile sensing scenarios due to the high mobility of users and users may not be aware of each other for privacy reasons. We consider an untrusted aggregator that is curious about each individual user's data. The aggregator may eavesdrop all the messages sent from/to every user. A number of users may collude with the aggregator, and reveal their data to the aggregator. A number of users may also collude to obtain the aggregate.

Encryption Scheme Module

One constructing block of our answer is the additive homomorphic encryption scheme. Encryption is the procedure of translating undeniable textual content records (plaintext) into some thing that seems to be random and meaningless (ciphertext). Decryption is the method of changing ciphertext lower back to plaintext. To encrypt extra than a small quantity of data, symmetric encryption is used. A *symmetric key* is used during both the encryption and decryption processes. To decrypt a particular piece of ciphertext, the key that was used to encrypt the data must be used.

The goal of every encryption algorithm is to make it as difficult as possible to decrypt the generated ciphertext without using the key. If a really good encryption algorithm is used, there is no technique significantly better than methodically trying every possible key. For such an algorithm, the longer the key, the more difficult it is to decrypt a piece of ciphertext without possessing the key. It is difficult to determine the quality of an encryption algorithm. Algorithms that look promising sometimes turn out to be very easy to break, given the proper attack. When selecting an encryption algorithm, it is a good idea to choose one that has been in use for several years and has successfully resisted all attacks.

Key Generation Module

Suppose there are nc random numbers. The aggregator has access to all the numbers, and it computes the sum of these numbers as the decryption key k_0 . These numbers are divided into n random disjoint subsets, each of size c . These n subsets are assigned to the n users, where each

user has access to one subset of numbers. User i computes the sum of the numbers assigned to it as the encryption key k_i . The aggregator cannot know any user's encryption key because it does not know the mapping between the random numbers and the users. When c is large enough, it is infeasible for the aggregator to guess the numbers assigned to a particular user with a brute-force method. The aggregator's decryption key cannot be revealed by any user because no user knows all the numbers.

Aggregation Protocol Module

The Min aggregate is defined as the minimum value of the users' data. This module presents a protocol that employs the Sum aggregate to get Min. Each user uses just one set of secrets for all instances of the sum aggregation protocol. When the plaintext space is large, the cost of the basic scheme is high. In some application scenarios, it may not be necessary to get the exact Min, but an approximate answer is good enough. For such scenarios, the basic scheme can be extended to get an approximate Min with much smaller cost.

6.0 Conclusion

This paper provides each user its own privacy with sum aggregation of individual user's data. The protocol uses HMAC based key management technique to provide efficient aggregation. This protocol will handle more users than existing system. Based on the Sum aggregation protocol, Min aggregate is calculated. To deal with dynamic leaves and joins the factors like density, distance is considered. The main aim of this project is to introduce a secure Multi sink Time Stamp Scheme. To achieve this, a powerful and secure Straw-Man key aggregation variant was extended to a multi-well parameter to create a multi-well timestamp scheme that offers a guaranteed tracking property.. The proposed Multi sink Time Stamp scheme was shown to satisfy all of the specified security requirements and fulfills the stronger break-resistant property. The Multilink Time Stamp aggregated Key scheme thus remains secure, even if the threshold cryptosystem has been broken, i.e., the group secret or individual secret shares are known or controlled by an adversary. The efficiency analysis showed that the proposed Multisink Time Stamp scheme outperforms other existing schemes and is optimal in terms of exponentiations with respect to threshold aggregated Key verification and near optimal for individual aggregated Key verification, while providing break resistance.

7.0 Acknowledgement

We would like to express our sincere gratitude Mr. Atul Marathe (Adjunct Professor), Dr. Ashok Saraf (Innovation Club Member) for their invaluable guidance and support throughout the research process. We also wish to thank Dr. Sunil B. Thakare (Principal, APCOER, Pune) for their support. Finally, we are grateful to all of the research participants who generously gave their time and effort to this project..

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] Verma, M. K., & Dhabliya, M. D. (2015). Design of Hand Motion Assist Robot for Rehabilitation Physiotherapy. International Journal of New Practices in Management and Engineering, 4(04), 07–11.
- [7] M. Jawurek and F. Kerschbaum, Sharing Decryption in the Context of Voting or Lotteries, Proc. 12th Privacy Enhancing Technologies Symp.(PETS 12), 2012.
- [8] M. Shao, Y. Yang, S. Zhu, and G. Cao, Towards Statistically Strong Source Anonymity for Sensor Networks, Proc. IEEE INFOCOM, 2008.
- [9] C. Castelluccia, Efficient Aggregation of Encrypted Data in Wireless Sensor Networks, Proc. Second Ann. Intl Conf. Mobile and Ubiquitous Systems: Networking and Services
- [10] 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.
- [11] Q. Li and G. Cao, Providing Privacy-Aware Incentives for Mobile Sensing, Proc. IEEE PerCom, 2013.
- [12] MNDOLI, “Mnosha Permissible Exposure Limits,” <http://www.dli.mn.gov/OSHA/PDF/pels.pdf>, 2013.
- [13] S.B. Eisenman, E. Miluzzo, N.D. Lane, R.A. Peterson, G.-S. Ahn, and A.T. Campbell, “The Bikenet Mobile Sensing System for Cyclist Experience Mapping,” Proc. ACM Fifth Int’l Conf. Embedded Networked Sensor Systems (SenSys ’07), pp. 87-101, 2007.
- [14] M.G. Apte, W.J. Fisk, and J.M. Daisey, “Indoor Carbon Dioxide Concentrations and SBS in Office Workers,” Proc. Healthy Buildings Conf., pp. 133-138, 2000.