ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

Comparative Study of Secure Verification System against Attacks in Mobile Sensing

B.Likitha Reddy[1], A.Rosline Mary[2], A. S Kavitha Bai[3]

U.G. Student, Department of CSE, Vemana Institute of Technology, Bangalore, India[1]

Asst. Professor, Department of CSE, Vemana Institute of Technology, Bangalore, India[2]

Asst. Professor, Department of CSE, Vemana Institute of Technology, Bangalore, India[3]

ABSTRACT: The increasing capabilities of mobile devices have given raise to many mobile sensing applications. The problem with existing system of the mobile sensing applications is that the sensor data aggregation assume a trusted aggregator, and hence cannot protect user privacy against untrusted aggregator. An untrusted aggregator in mobile sensing can periodically obtain desired statistics over the data contributed by multiple mobile users, without compromising the privacy of each user. To address this problem, we propose an efficient protocol to obtain the Sum aggregate, which employs an additive homomorphic encryption and a novel key management technique. Evaluations show that our protocols are orders of magnitude faster than existing solutions, and it has much lower communication overhead.

KEYWORDS: Mobile Sensing, Privacy, Data Aggregator, Key Management

I. INTRODUCTION

Most mobile devices such as smart phones are equipped with a rich set of embedded sensors such as camera, microphone, GPS, accelerometer, ambient light sensor, gyroscope, and so on have created a huge opportunity of sensing. This enables various mobile sensing applications such as environmental monitoring, traffic monitoring, healthcare, and so on by collecting data through mobile devices and utilizing the data to obtain rich information about people and their surroundings. In many scenarios, aggregation statistics need to be periodically computed from a stream of data contributed by mobile users, to identify some phenomena or track some important patterns. For example, to monitor the propagation of a new flu and count the number of users infected by this flu ("1" if infected and "0" otherwise). However, this aggregation of statistics is hindered by obstacles.

- An untrusted aggregator can periodically obtain desired statistics over the data contributed by multiple mobile users, without compromising the privacy of each user. To address this problem they design encryption schemes in which the aggregator can only decrypt the sum of all users' data but nothing else.
- 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. Also, 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.

To address this problem we propose a construction that does not require bidirectional communications between the aggregator and the users, but it has high computation and storage cost to deal with collusions in a large system.

We propose a new protocol for mobile sensing to obtain the sum aggregate of time series data in the presence of an untrusted aggregator. Our protocol employs an additive homomorphic encryption and a novel key management scheme based on efficient HMAC to ensure that the aggregator can only obtain the sum of all users' data, without knowing individual user' data or intermediate result. In our protocol, each user (the aggregator) only needs to compute a very small number of HMACs to encrypt her data (decrypt the sum). Hence, the computation cost is very low. Another nice property of our protocol is that it only requires a single round of user-to-aggregator communication. Our protocols for Sum can be easily adapted to derive many other aggregate statistics such as Count and Average.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

The remainder of this paper is organized as follows. Section II presents Literature Survey. Section III presents the existing privacy aware data aggregation in mobile sensing. Section IV presents the proposed secure verification system against attacks in mobile sensing. The last section conclude the paper.

II.LITERATURE SURVEY

Many works have addressed various security and privacy issues in mobile sensing networks and systems but they do not consider data aggregation. To achieve privacy preserving sum aggregation of time series data, Rastogi and Nath[1] designed an encryption scheme where the decryption key is divided into portions. They proposed private aggregation algorithm for distributed time-series data that offers good practical utility without any trusted server. 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.

Rieffel et al [2] proposed how an untrusted data aggregator can learn desired statistics over multiple participants' data, without compromising each individual's privacy. We 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.Li and Cao [3] proposed a privacy-aware incentive scheme, to stimulate user participation, the scheme rewards users with credits for their contributed data without revealing what data a user has contributed but it is designed for single-report tasks and has high computation and communication cost.

III.EXISTING SYSTEM

Most previous works on sensor data aggregation assume a trusted aggregator, and hence cannot protect user privacy against an untrusted aggregator in mobile sensing applications. Q.Li and G.Cao et al [4], Sensor data aggregation assumes an untrusted 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.

IV.PROPOSED SYSTEM

We propose a new privacy-preserving protocol to obtain the Sum aggregate of time series data is illustrated in Fig 1. The protocol utilizes additive homomorphic encryption and a novel, HMAC- based key management technique to perform extremely efficient aggregation. An aggregator wishes to get the aggregate statistics of n mobile users periodically for example every one hour. The key dealer assigns keys to each user and the aggregator.

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

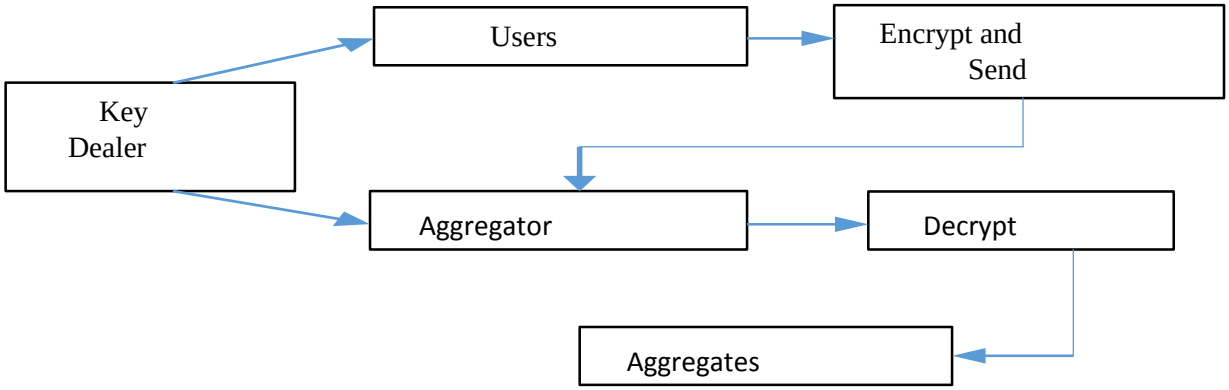

Fig 1.Proposed System for Secure Verification in Mobile Sensing

Each user encrypts her data xi with key ki and sends the cipher text to the aggregator. From the cipher texts of the users, the aggregator decrypts the Sum aggregate statistics using the aggregator encryption key k0.

Sum Aggregation Protocol
Setup: The key dealer assigns a set of secret values to each user (a subset) and the aggregator (nc numbers).

Notations:
i - user' key
xi –user data
M- $2[\log_2(n\Delta)]$
Δ - The maximum value of user's data
M- number of users in the system
Ci - cipher text
ϒ - The Maximum fraction of user that collude with the adversary
C - The number of secrets assigned to each user in the protocol
q - The number of secrets assigned to the aggregator in the protocol.

User:
Enc: Each user i generates encryption key ki using the secret values assigned to it. It encrypts its data xi by computing ci = (ki+xi) mod M and sends the cipher text to the aggregator.

Aggregator:
Decrypts sum aggregate S$= \sum_{i=1}^{n} xi$ by computing, S $= (\sum_{i=1}^{n} ci - ko)\ mod\ m$
The aggregator can get the correct sum only if the following equation holds
ko = $(\sum_{i=1}^{n} ki)\ mod\ m$

V.KEY GENERATION

A Straw-Man Construction for Key Generation
Consider there are nc random numbers. The aggregator has access to all the numbers and computes the sum of these numbers as the decryption key k0. These numbers are divided into n random disjoint subsets each of size c. These n subsets are assigned to n users where each user has access to one subset of numbers. User i computes the sum of these numbers assigned to it as encryption key k_i. Our Construction for Key Generation to reduce the computation overhead at the aggregator. Consider,

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

$a_1 + a_2 + \ldots + a_{nc} = a_1 + a_2 + \ldots + a_{nc}$

If we remove nc-q summands from the right hand side and subtract them from the left hand side, the derived equation is $a_1 + \ldots + a_{nc} + (-a_1) + \ldots + (-a_{nc-q}) = a_{nc-q+1} + \ldots + a_{nc}$

which is equivalent to the original equation. By removing some summands from the aggregator side and subtracting them from the user side will result in aggregator having to generate less summands and hence less computation overhead. This also provides better security for the users. Each user generates more summands and hence it is difficult to guess the summands generated by each user.

Table 1

The Computation Cost of Proposed Construction and Straw- Man Construction for 80-bit Security when ϒ=0.1

	n	10^2	10^3	10^4	10^5	10^6
User	Straw man	11	8	6	5	4
	Proposed	12	10	8	6	6
Aggregator	Straw man	1100	8000	6.10^4	5.10^5	4.10^6
	Proposed	13	8	6	5	4

Table 2 compares our construction to the straw-man construction in security and cost. When the total computation cost (for users and the aggregator) is the same, our construction achieves better security. Also, it has smaller computation cost at the aggregator. Upon initial inspection, our construction may seem to doublethe computation cost at each user (i.e., from c to roughly2c). In practice, however, it can use a smaller c to achievethe same security level. Table 1 shows the computationcost of the two constructions at the same security level. For a wide range of $n(10^2\text{-}10^6)$, the computation cost at each user is slightly higher in our construction, but the computation cost at the aggregator is orders of magnitude smaller.

Table 2

The Security and Cost of Proposed Construction and the Straw-Man Construction

	Straw man	Proposed System
p_b	$\frac{1}{\binom{(1-\gamma)nc}{c}}$	$\frac{1}{\binom{(1-\gamma)nc}{c}\cdot\binom{(1-\gamma)n(c-1)}{c-1}}$
Comp. (Total)	$2nc$	$2nc$
Comp. (user)	c	$2c\text{-}\frac{q}{n}$
Comp. (Aggregator)	nc	$q(q<n)$
Storage (User)	c	$2c\text{-}q$
Storage. (Aggregator)	nc	q

VI.EXPERIMENTAL RESULTS

The appropriate screen shots of the proposed system are shown below.The user first has to register with a valid email id as illustrated in Fig 2. The user then receives a group key to his email id, using which he can login, before which the

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

aggregator activates the user. The registered user can login and can to do operations such as upload a file, download a file, etc. For the upload operation by the user, the user has to encrypt the file, this is illustrated in Fig 3. The aggregator can view the user details, the files uploaded by the user etc.

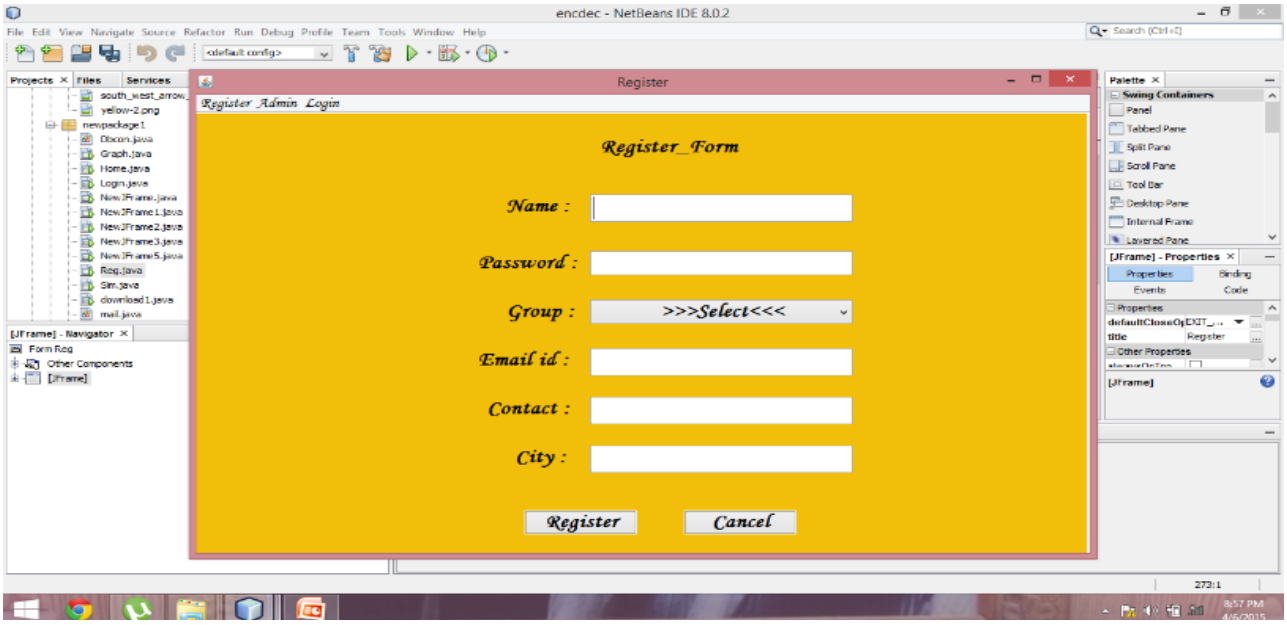

Fig 2: The registration form for the new user to register with valid email id.

The user first has to register with a valid email id as illustrated in Fig 2. The user then receives a group key to his email id, using which he can login, before which the aggregator activates the user. The registered user can login and can to do operations such as upload a file, download a file, etc. For the upload operation by the user, the user has to encrypt the file, this is illustrated in Fig 3. The aggregator can view the user details, the files uploaded by the user etc.

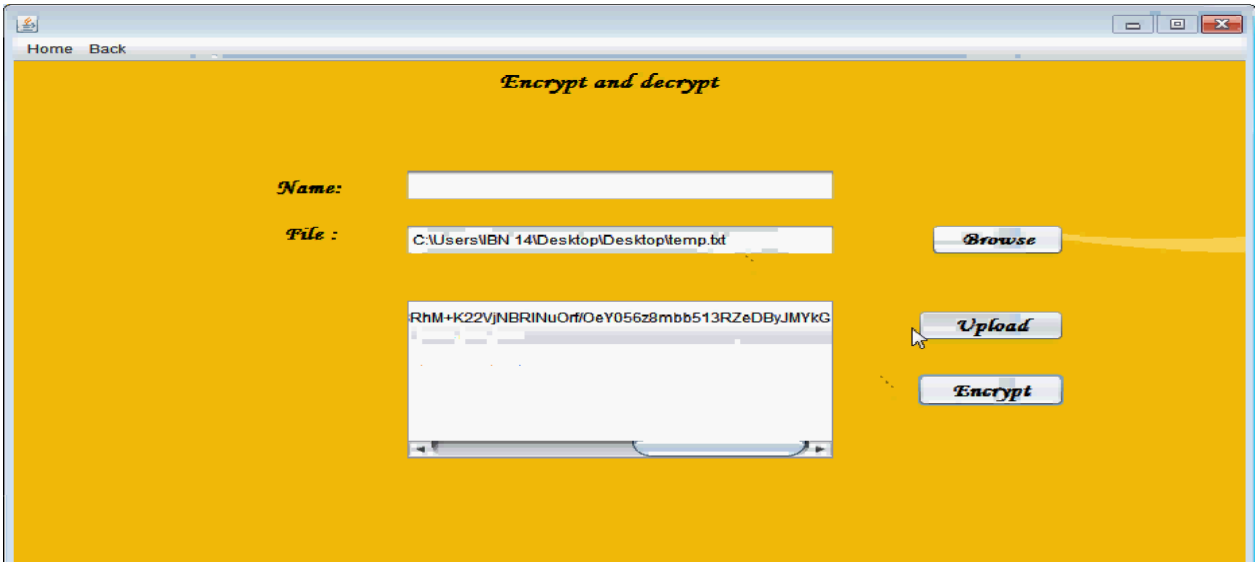

Fig 3: Encrypt and Decrypt data

ISSN(Online): 2319 - 8753
ISSN (Print) :2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 5, May 2015

VII.CONCLUSION

The collect useful aggregate statistics in mobile sensing without leaking mobile users' privacy, we proposed a new privacy preserving protocol to obtain the Sum aggregate of time-series data. The protocol utilizes additive holomorphic encryption and a novel, HMAC based key management technique to perform extremely efficient aggregation.Implementation-based measurements show that operations at user and aggregator in our protocol are orders of magnitude faster than existing work. Thus, our protocol can be applied to a wide range of mobile sensing systems .

REFERENCES

[1].V. Rastogi and S. Nath, "Differentially Private Aggregation of Distributed Time-Series with Transformation and Encryption," Proc. ACM SIGMOD Int'l Conf. Management of Data, 2010.

[2] E.G. Rieffel, J. Biehl, W. van Melle, and A.J. Lee, "Secured Histories Computing Group Statistics on Encrypted Data While Preserving Individual Privacy," http://arxiv.org/abs/1012.2152,2010.

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

[4] Q. Li and G. Cao, "Efficient and Privacy-Preserving Data Aggregation in Mobile Sensing," Proc. IEEE ICNP, pp. 1-10, 2012